数理科学シリーズ
7

数理論理学 語の問題

イリノイ大学教授
理学博士 竹内外史
著

培風館

まえがき

10年ほど前に，数理科学シリーズの中の1巻として「数理論理学」もまとめようという計画があり，全体を4章に分け，著者はその第4章担当ということになっていた。

昨年の5月になり，培風館から各章を別々の本にしたいと思うが，執筆願えるだろうかといわれたときは寝耳に水といった感じであった。さらに，第4章の予定が‘語の問題’だというので驚いた。どうしてこういう専門外のものを引き受けることになったのだろうか。いまとなっては見当もつかないが，その当時，ほかに専門家がいたわけでもないし，第1章から第3章までの執筆予定者がいずれも多忙なる面々だったので，どうせ無限遠の未来に属することと気楽な気持で引き受けたものと思われる。

ところで，その無限遠の未来が突然現在にかわってとまどいを感じないわけにゆかなかった。引き受けたものだろうか，それとも断わったほうが良心的だろうか，といろいろのことが考えられた。しかし，語の問題は数理論理学を専門としない一般数学者が数理論理学の分野でいちばん興味をもつところであるから，これについて手軽な小冊子をかいてその好奇心に応えるのは，数理論理学に働くものが一般数学者にすべき，よきサービスであるように思われた。

さらに，数理科学シリーズの1巻として‘語の問題’についてかくとすれば，いろいろのことが考えられた。しかし，この本ではあまり欲ばらずに，この分野でいちばん中心的でおもしろい2つの問題——ヒルベルトの第10問題と群の語の問題——にしぼることにした。このため，この本の体裁は，あまり余計なことにかえりみず，まっしぐらに問題に直進するというスタイルになっている。しかし，この分野ではこれがいちばん手っとり早い方法とも考えられる。

第1章に，帰納的関数の一般論について述べた。本当はこのシリーズに帰納的関数論も予定されていたのであるが，いまのところその見通しもつかないので，必要な基本的な事項をここに載せることにした。このことに興味をもたれ

る方は，まとまった成書を読まれることをお勧めする。

第2章と第3章は，いずれも第1章を用いるが，お互いに独立にかかれているので，第2章の前に第3章から読み始めてもよい。第3章で，自由群のことについて述べたが，だいたい数学的素養のある方に全体の様子がわかるようにというつもりであり，もちろん自由群を理解するためには不満足きわまりないものである。

この書が大方の好奇心を大幅に満たすことになれば，著者としてはこれ以上の喜びはない。

本書は，1972年の夏休みの一部をさいてかかれた。成書としての体裁上，もう少し内容を増やしてほしいという出版社の強い要請があり，ふやすべきものもないではなかったが，これ以上の時間をさく余裕が筆者にはなかったため，このままで出版することを希望した。この希望を快く受け入れられて出版に努力，原稿の整理，校正等に多大の努力を払われた培風館の牧野末喜氏に，ここに心からの感謝の意を表したい。

1973 年 1 月

イリノイにて

竹内　外史

目　次

はしがき

第1章　帰納的関数　1～41

1·1　自然数について　1
1·2　原始帰納的関数　6
1·3　帰納的関数　15
1·4　帰納的可算について　22
1·5　ゲーデル数　29
1·6　truth definition　36
1·7　決定問題への応用　39

第2章　ヒルベルトの第10問題　42～66

2·1　第10問題　42
2·2　初等的命題　43
2·3　diophantine の基本的性質　45
2·4　方程式 $x^2-(a^2-1)y^2=1$ の解　46
2·5　$v=y_u(a)$ は diophantine である　53
2·6　$\alpha=\beta^u$ は diophantine である　57
2·7　$y=x!$ は diophantine である　59
2·8　重要な補助定理　61

第3章　群の語の問題　67～111

3·1　自由群　67
3·2　関係のある群　73
3·3　融合積　75
3·4　有限表示群　80
3·5　Higman 群　82
3·6　benign について　87
3·7　重要な補助定理　95
3·8　補助定理の証明　104

参考文献 113～114
索　　引 115～116
記号一覧 117～118

第 1 章

帰納的関数

1・1　自然数について

この本では，有理整数というのは

$$0,\ \pm1,\ \pm2,\ \pm3,\ \cdots$$

のことで，自然数というのは

$$0,\ 1,\ 2,\ 3,\ \cdots$$

のことであるとする。断わらないかぎりは，いつでも自然数のことを考えることにする。たとえば，何の断わりもなく変数を用いたら，それは自然数についての変数であると思うことにする。

論理記号は

$\neg$	（でない）	$\wedge$	（そして）
$\vee$	（または）	$\rightarrow$	（ならば）
$\forall$	（すべて）	$\exists$	（存在する）

を用いる。論理記号の用い方は一通り知っているものとする。

‘A と B は同値である’

を

$$A \leftrightarrow B$$

で表わす。これは

$$(A \rightarrow B) \wedge (B \rightarrow A)$$

の略であると思えばよい。

$$\forall x \leq a A(x)$$

は

$$\forall x(x \leq a \rightarrow A(x))$$

の略であり

$$\exists x \leq a A(x)$$

は

$$\exists x(x \leq a \wedge A(x))$$

の略である。

$$\forall x < a A(x), \qquad \exists x < a A(x)$$

も同様に定義される。また

$$\neg \forall x < a A(x) \leftrightarrow \exists x < a \neg A(x)$$

$$\neg \exists x < a A(x) \leftrightarrow \exists x < a \neg A(x)$$

などが成立する。

$\forall x_1 \forall x_2 \cdots \forall x_n A(x_1, x_2, \cdots, x_n)$ を

$$\forall x_1, \cdots, x_n A(x_1, \cdots, x_n)$$

と略記し，$\exists x_1 \exists x_2 \cdots \exists x_n A(x_1, x_2, \cdots, x_n)$ を

$$\exists x_1, \cdots, x_n A(x_1, \cdots, x_n)$$

と略記する。

a が b の約数であることを

‘a が b を割る’

といって

$$a \mid b$$

とかく。そうでないとき

$$a \nmid b$$

とかく。

a と b との最大公約数を

$$(a, b)$$

で表わし，$(a, b)=1$ のとき

$$\text{‘}a \text{ と } b \text{ は互いに素である’}$$

という。

a と b との順序対は，上の (a, b) と区別するために

$$\langle a, b\rangle$$

で表わすことにする。

$a \dot{-} b$ を，$b \leq a$ のときは普通の $a-b$ を，そうでないときは0を表わすものと定義する。

$$a \equiv b \quad (\mathrm{mod}\, c)$$

とは

$$(c | b \dot{-} a) \wedge (c | a \dot{-} b)$$

のことである。論理記号を用いてかけば

$$a | b \quad \text{は} \quad \exists x(ax = b)$$

$$a \equiv b \ (\mathrm{mod}\, c) \quad \text{は} \quad \exists x(a = b + cx \vee b = a + cx)$$

となる。

つぎの初等整数論の簡単な定理は，どういうわけか英語では Chinese remainder theorem とよばれている。この本では，単に剰余定理とよぶことにする。

剰 余 定 理

$m_1, m_2, \cdots, m_n$ は互いに素とする。すなわち，$i \neq j$ ならば $(m_i, m_j) = 1$ とする。このとき，任意の $a_1, a_2, \cdots, a_n$ に対して，ある a が存在して

$$a \equiv a_1 \quad (\mathrm{mod}\, m_1)$$

$$a \equiv a_2 \quad (\mathrm{mod}\, m_2)$$

$$\vdots$$

$$a \equiv a_n \quad (\mathrm{mod}\, m_n)$$

を満たす。

つぎに，自然数全体の集合を N としたとき，N の二重対全体の集合 $N\times N$ からNへの bijection (1対1で onto な写像)を簡単につくることを考えよう。

いま，求めるものを

$$J: N\times N\to N$$

とすれば，Jは2変数の関数

$$J(a, b)$$

であって，a, b は自然数を走るものとしてよい。いちばん簡単なものとして，つぎの図で示すようなものを考えよう。

a \ b	0	1	2	3	4	5	6	7
0	0	1	3	6	10	15	21	
1	2	4	7	11	16	22		
2	5	8	12	17	23			
3	9	13	18	24				
4	14	19	25					
5	20	26						
6	27							

この図から，どのようなJをつくろうとしているのかを考えてみる。ここで，Jが $N\times N$ から N への bijection になっていることなどは明らかであろう。

この並べ方をみると，$J(a, b)$ に対して

(i)　$a_1+b_1<a_2+b_2\to J(a_1, b_1)<J(a_2, b_2)$

(ii)　$a_1+b_1=a_2+b_2$, $a_1<a_2\to J(a_1, b_1)<J(a_2, b_2)$

の2条件が満たされていることがただちにわかる。

いま，$x+y<n$ になるような $\langle x, y\rangle$ の個数を数えてみれば，明らかに

$$1+2+\cdots+n=\frac{1}{2}n(n+1)$$

となる。この中に0もはいっているから，それまでに用いられていない数の最小は

$$\frac{1}{2}n(n+1)$$

である。

ところで，$\langle a, b\rangle$ は，$a+b=n$ となるものの中では a の大きさで比べられるから

$$J(a, b)=\tfrac{1}{2}(a+b)(a+b+1)+a$$

となる。

いま，n 変数の関数 g，$n+2$ 変数の関数 h が与えられたときに

$$\text{I}\qquad \begin{cases} f(0, x_1, \cdots, x_n)=g(x_1, \cdots, x_n) \\ f(x+1, x_1, \cdots, x_n)=h(f(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n) \end{cases}$$

の2つの条件を満たす関数 f のことを g と h からIで定義される関数という。

この定義が妥当であることは，つぎの定理から明らかであろう。

定理 1　g を n 変数の関数，h を $n+2$ 変数の関数とするとき，Iで定義される f がただ一通り存在する。

[証明]　まず，ただ一通りであることは，f_1，f_2 がともにIを満たすとするとき

$$f_1(x, x_1, \cdots, x_n)=f_2(x, x_1, \cdots, x_n)$$

が x についての数学的帰納法で容易に証明されることから明らかである。

つぎに，Iを満たす f が存在することを証明しよう。

$$P(y, x, x_1, \cdots, x_n)$$

を $x=0$ ならば

$$g(x_1, \cdots, x_n)=y$$

$x=n+1$ ならば，a_0，a_1，$\cdots$，a_n なる点列で

$$a_0=g(x_1, \cdots, x_n)$$
$$a_{i+1}=h(a_i, i, x_1, \cdots, x_n) \qquad (0\leq i<n)$$

を満たすものが存在して

$$y=h(a_n, n, x_1, \cdots, x_n)$$

と定義すれば

'$P(y, x, x_1, \cdots, x_n)$ なる y がただ1つ存在する'

が x についての数学的帰納法で容易に証明されることからわかる。

よって，$f(x, x_1, \cdots, x_n)$ を，$P(y, x, x_1, \cdots, x_n)$ を満たす y と定義すれば

よい。

1·2　原始帰納的関数

f が原始帰納的関数(primitive recursive function)であるということをつぎのように定義する。

1·2·1
$$f(x)=0$$
であれば，f は原始帰納的関数である。

1·2·2
$$f(x)=x+1$$
であれば，f は原始帰納的関数である。

1·2·3
$$f(x_1,\ \cdots,\ x_n)=x_i \qquad (1\leq i\leq n)$$
であれば，f は原始帰納的関数である。

1·2·4　$g,\ h_1,\ \cdots,\ h_m$ が原始帰納的関数であって
$$f(x_1,\ \cdots,\ x_n)=g(h_1(x_1,\ \cdots,\ x_n),\ \cdots,\ h_m(x_1,\ \cdots,\ x_n))$$
であれば，f も原始帰納的関数である。

1·2·5　g と h が原始帰納的関数であって，f が 1·1 節の I で定義された関数であれば，f も原始帰納的関数である。

1·2·6　1·2·1〜1·2·5 の条件でつくられた関数だけが原始帰納的関数である。

さて，原始帰納的関数の性質になれるために，まずいろいろな原始帰納的な関数を求めてみる。

最初に，$f(x_1,\ \cdots,\ x_n)=k$ という関数が原始帰納的であるということは，1·2·1，1·2·2，1·2·3 から明らかであることを注意した上で求めてみる。

1·2·7　$a+b$ は原始帰納的関数である($a,\ b$ の 2 変数の関数である)。

[証明]　‘＋’は
$$a+0=a$$
$$a+(b+1)=(a+b)+1$$
を満たすから，これは
$$g(a)=a, \qquad h(y,\ b,\ a)=y+1$$

として，Ⅰで定義された関数である。ゆえに，原始帰納的関数である。

1·2·8　$a \cdot b$ は原始帰納的関数である。

[証明]　$a \cdot b$ は

$$a \cdot 0 = 0$$

$$a \cdot (b+1) = a \cdot b + a$$

を満たすから，原始帰納的関数である。

1·2·9　a^b は原始帰納的関数である。

[証明]

$$a^0 = 1$$

$$a^{(b+1)} = a^b \cdot a$$

より明らか。

1·2·10　$a!$ は原始帰納的関数である。

[証明]

$$0! = 1$$

$$(a+1)! = a!(a+1)$$

1·2·11　$a \dot{-} 1$ は原始帰納的関数である。

[証明]

$$0 \dot{-} 1 = 0$$

$$(a+1) \dot{-} 1 = a$$

1·2·12　$a \dot{-} b$ は原始帰納的関数である。

[証明]

$$a \dot{-} 0 = a$$

$$a \dot{-} (b+1) = (a \dot{-} b) \dot{-} 1$$

1·2·13　$\min(a, b)$ は原始帰納的関数である（$\min(a, b)$ は a と b との小さいほうを意味する）。

[証明]

$$\min(a, b) = b \dot{-} (a \dot{-} b)$$

1·2·14　$\min(a_1, \cdots, a_n)$ は原始帰納的関数である（$\min(a_1, \cdots, a_n)$ は $a_1, \cdots, a_n$ の最小）。

[証明]　$\min(a_1, \cdots, a_n) = \min(\cdots, \min(\min(a_1, a_2), a_3), \cdots, a_n)$

1·2·15　$\max(a, b)$ は原始帰納的関数である（$\max(a, b)$ は a と b との大きいほうを意味する）。

[証明]

$$\max(a, b) = (a+b) \dot{-} \min(a, b)$$

1·2·16　$\max(a_1, \cdots, a_n)$ は原始帰納的関数である。

[証明]　$\max(a_1, \cdots, a_n)=\max(\cdots, \max(\max(a_1, a_2), a_3), \cdots, a_n)$

1·2·17　$\mathrm{sg}(a)$ を

$$\mathrm{sg}(a)=\begin{cases} 0 & (a=0) \\ 1 & (a\neq 0) \end{cases}$$

と定義すれば，$\mathrm{sg}(a)$ は原始帰納的関数である。

[証明]

$$\mathrm{sg}(0)=0$$
$$\mathrm{sg}(a+1)=1$$

これが1·1節のⅠの形であることに注意せよ。

1·2·18　$\overline{\mathrm{sg}}(a)$ を

$$\overline{\mathrm{sg}}(a)=\begin{cases} 1 & (a=0) \\ 0 & (a\neq 0) \end{cases}$$

と定義すれば，$\overline{\mathrm{sg}}(a)$ は原始帰納的関数である。

[証明]

$$\overline{\mathrm{sg}}(0)=1$$
$$\overline{\mathrm{sg}}(a+1)=0$$

1·2·19　$|a-b|$ は原始帰納的関数である。

[証明]　$$|a-b|=(a\dot{-}b)+(b\dot{-}a)$$

1·2·20　$\mathrm{rm}(a, b)$ は原始帰納的関数である。

[証明]　$\mathrm{rm}(0, b)=0$

$$\mathrm{rm}(a+1, b)=(\mathrm{rm}(a, b)+1)\cdot\mathrm{sg}(|b-(\mathrm{rm}(a, b)+1)|)$$

1·2·21　$[a/b]$ を，a を b で割ったときの商とすれば，$[a, b]$ は原始帰納的関数である。

[証明]　$$[0/b]=0$$

$$[(a+1)/b]=[a/b]+\overline{\mathrm{sg}}(|b-(\mathrm{rm}(a, b)+1)|)$$

いま，$\sum_{y<z} f(x_1, \cdots, x_n, y)$ を $z=0$ のときは0として

$$\sum_{y<(a+1)} f(x_1, \cdots, x_n, y)=(\sum_{y<a} f(x_1, \cdots, x_n, y))+f(x_1, \cdots, x_n, a)$$

によって定義すれば，この定義自身1·1節のⅠの形であるから，つぎの性質が成立する。

1·2·22　f が原始帰納的関数であれば

$$\sum_{y<z} f(x_1, \cdots, x_n, y)$$

も原始帰納的関数である。

つぎに，$\prod_{y<z} f(x_1, \cdots, x_n, y)$ を，$z=0$ のときは 1 として

$$\prod_{y<(a+1)} f(x_1, \cdots, x_n, y) = \Big(\prod_{y<a} f(x_1, \cdots, x_n, y)\Big) \cdot f(x_1, \cdots, x_n, a)$$

と定義すれば，1·2·22 と同様にして，つぎの性質が成り立つ。

1·2·23　f が原始帰納的関数であれば

$$\prod_{y<z} f(x_1, \cdots, x_n, y)$$

も原始帰納的関数である。

いま，$P(x_1, \cdots, x_n)$ が $x_1, \cdots, x_n$ についての命題であるとき，$f(x_1, \cdots, x_n)$ が $P(x_1, \cdots, x_n)$ の**特性関数**であるというのは

$$P(x_1, \cdots, x_n) \leftrightarrow f(x_1, \cdots, x_n)=0$$

$$\neg P(x_1, \cdots, x_n) \leftrightarrow f(x_1, \cdots, x_n)=1$$

の 2 つの条件が成立することをいう。

'$P(x_1, \cdots, x_n)$ が原始帰納的関数である'

ということを，P の特性関数が原始帰納的関数であることと定義しよう。

1·2·24　$a=b$ は原始帰納的関数である。

[証明]　$a=b$ の特性関数は $\mathrm{sg}|a-b|$ である。

1·2·25　P, Q が原始帰納的関数ならば

$$\neg P,\quad P \wedge Q,\quad P \vee Q,\quad P \rightarrow Q,\quad P \leftrightarrow Q$$

も原始帰納的関数である。

[証明]　P, Q の特性関数をそれぞれ f, g とすれば，$\neg P$ の特性関数は $\overline{\mathrm{sg}}(f)$ であり，$P \vee Q$ の特性関数は $f \cdot g$ である。

$P \wedge Q$, $P \rightarrow Q$, $P \leftrightarrow Q$ は，$\neg$ と $\vee$ を組み合わせてできるからよい。

1·2·26　P が原始帰納的関数ならば

$$\exists y<z P(x_1, \cdots, x_n, y) \quad と \quad \forall y<z P(x_1, \cdots, x_n, y)$$

も原始帰納的関数である。

[証明]　P の特性関数を f とすれば，$\exists y<zP(x_1, \cdots, x_n, y)$ の特性関数は

$$\prod_{y<z} f(x_1, \cdots, x_n, y)$$

となるからよい。　$\forall y<zP(x_1, \cdots, x_n, y)$ は，　$\neg\exists y<z\neg P(x_1, \cdots, x_n, y)$ と表わされるからよい。

いま，$\mu yP(y)$ を

$$\mu yP(y)=\begin{cases} P(y)\text{ を満たす } y \text{ があればその最小} \\ \text{なければ } 0 \end{cases}$$

と定義する。$\mu y<zP(y)$ を

$$\mu y(y<z \wedge P(y))$$

と定義する。

1·2·27　P が原始帰納的関数ならば

$$\mu y<zP(x_1, \cdots, x_n, y)$$

も原始帰納的関数である。

[証明]　$P(x_1, \cdots, x_n, y)$ の特性関数を $f(x_1, \cdots, x_n, y)$ とし，これらをそれぞれ $P(y)$, $f(y)$ と略記することにしよう。このとき

$$g(z)=\prod_{y\leq z} f(y)$$

すなわち

$$=\prod_{y<(z+1)} f(y)$$

とすれば，つぎのことが成立する。

z	0, 1, 2, 3, $\cdots$, k, $k+1$, $\cdots\cdots$
$P(z)$	←—— 偽 ——→ 真, $\cdots\cdots$
$f(z)$	1, 1, 1, 1, $\cdots$, 1, 0, $\cdots\cdots$
$g(z)$	1, 1, 1, 1, $\cdots$, 0, 0, 0, $\cdots\cdots$

したがって

$$h(z)=\sum_{y<z} g(y)$$

ととれば

$$\begin{array}{ll} z & 0,\ 1,\ 2,\ \cdots\cdots,\ k,\ k+1,\ \cdots\cdots \\ P(z) & \longleftarrow \text{偽} \longrightarrow \text{真},\ \cdots\cdots \\ h(z) & 0,\ 1,\ 2,\ \cdots\cdots,\ k,\ k,\ \cdots\cdots \end{array}$$

となる。ゆえに，求める $\mu y<zP(y)$ の特性関数は，つぎのようになる。

$$\mathrm{sg}(z-\mathrm{sg}(f(z))\cdot h(z))h(z)$$

1·2·28　$f,\ g$ が原始帰納的関数ならば

$$f(x_1,\ \cdots,\ x_n)=g(x_1,\ \cdots,\ x_n)$$

も原始帰納的関数である。

[証明]　$f(x_1,\ \cdots,\ x_n)=g(x_1,\ \cdots,\ x_n)$ の特性関数は，つぎのようになる。

$$\mathrm{sg}|f(x_1,\ \cdots,\ x_n)-g(x_1,\ \cdots,\ x_n)|$$

1·2·29　$a<b$ は原始帰納的関数である。

[証明]　$$a<b \leftrightarrow \exists x<b(a+(x+1)=b)$$

$Q_1,\ \cdots,\ Q_m$ が互いに相反する命題であるということを，$i \neq j$ に対して

$$\forall x_1,\ \cdots,\ x_n \neg(Q_1(x_1,\ \cdots,\ x_n)\wedge Q_2(x_1,\ \cdots,\ x_n))$$

が成立していることと定義する。

いま，$Q_1,\ \cdots,\ Q_m$ が互いに相反する命題であって，$\varphi_1,\ \cdots,\ \varphi_{m+1}$ が関数であるとき，新しい関数 φ を

$$\varphi(x_1,\ \cdots,\ x_n)=\begin{cases} \varphi_1(x_1,\ \cdots,\ x_n) & (Q_1(x_1,\ \cdots,\ x_n)\ \text{が成立するとき}) \\ \varphi_2(x_1,\ \cdots,\ x_n) & (Q_2(x_1,\ \cdots,\ x_n)\ \text{が成立するとき}) \\ \vdots & \\ \varphi_m(x_1,\ \cdots,\ x_n) & (Q_m(x_1,\ \cdots,\ x_n)\ \text{が成立するとき}) \\ \varphi_{m+1}(x_1,\ \cdots,\ x_n) & (\text{以上のいずれでもないとき}) \end{cases}$$

によって定義することを $Q_1,\ \cdots,\ Q_m$ の場合に分けて，φ を $\varphi_1,\ \cdots,\ \varphi_{m+1}$ で定義するという。

1·2·30　f を $Q_1,\ \cdots,\ Q_m$ の場合に分けて，$f_1,\ \cdots,\ f_{m+1}$ で定義し

$$Q_1,\ \cdots,\ Q_m,\ f_1,\ \cdots,\ f_{m+1}$$

がすべて原始帰納的関数ならば，f も原始帰納的関数である。

[証明]　$Q_1, \cdots, Q_m$ の特性関数を $q_1, \cdots, q_m$ とすれば

$$f=\overline{\mathrm{sg}}(g_1)f_1+\cdots+\overline{\mathrm{sg}}(g_n)f_m+g_1+\cdots+g_m\cdot f_{m+1}$$

が成立するからよい。

1・2・31　$a \mid b$ は原始帰納的関数である。

[証明]　$$a \mid b \leftrightarrow \exists x<(b+1) \quad (ax=b)$$

1・2・32　$Pr(a)$ を ‘a は素数である’ ということにすれば，Pr は原始帰納的関数である。

[証明]　$$Pr(a) \leftrightarrow 1<a \wedge \forall x<a(1<x \rightarrow x \nmid a)$$

1・2・33　p_i を $(i+1)$ 番目の素数とする。すなわち

$$p_0=2,\ p_1=3,\ p_2=5,\ \cdots$$

とすれば，p_i は i の関数として原始帰納的関数である。

[証明]　$$p_0=2$$

$$p_{i+1}=\mu x<(p_i)!+2(p_i<x \wedge Pr(x))$$

われわれは a を素因数分解して

$$a=p_0{}^{a_0}\cdot p_1{}^{a_1}\cdots p_i{}^{a_i}\cdots$$

とする。ここに，$p_i \nmid a$ のときは $a_i=0$ とおくわけである。このとき，$(a)_i=a_i$ によって $(a)_i$ を定義することにする。すなわち，$(a)_i$ は，p_i が何乗 a にはいっているかという数である。

1・2・34　$(a)_i$ は原始帰納的関数である。

[証明]　$$(a_i)=\mu x<a(p_i{}^x \mid a \wedge p_i{}^{x+1} \nmid a)$$

$((a)_i)_j$ を $(a)_{i,j}$，$(((a)_i)_j)_k$ を $(a)_{i,j,k}$ というようにかくことにする。

a を素因数分解して

$$a=p_{i_1}{}^{n_1}\cdots p_{i_k}{}^{n_k}$$

とする。ここで，$n_j \neq 0$ とする。このとき，a を $n_1, \cdots, n_k$ なる系列を表わすものと思って，k のことを a の**長さ**といい

$$\mathrm{lh}(a)$$

で表わすことにする。

1·2·35　$\mathrm{lh}(a)$ は原始帰納的関数である。

[証明]　まず，$\mathrm{lh}(i, a)$ を

$$\mathrm{lh}(0, a)=0$$

$$\mathrm{lh}(i+1, a)=\begin{cases} \mathrm{lh}(i, a)+1 & (p_i \mid a \text{ のとき}) \\ \mathrm{lh}(i, a) & (\text{そうでないとき}) \end{cases}$$

と定義すれば

$$\mathrm{lh}(a)=\mathrm{lh}(a, a)$$

となる。

いま，正の自然数の有限列 $a_0, \cdots, a_s$ があったとき，この有限列を

$$a=p_0{}^{a_0}\cdots p_s{}^{a_s}$$

で表わせば，$\mathrm{lh}(a)$ は $s+1$ を表わすことになる。別の正の自然数の有限列 $b_0, \cdots, b_t$ を表わす自然数を b とするとき，$a_0, \cdots, a_s, b_0, \cdots, b_t$ なる自然数を表わす自然数を

$$a*b$$

とおくことにする。

1·2·36　$a*b$ は原始帰納的関数である。

[証明]

$$a*b=a\cdot\prod_{i<\mathrm{lh}(b)} p_{\mathrm{lh}(a)+i}^{(b)_i}$$

1·1 節の I は，$f(x+1, x_1, \cdots, x_n)$ を

$$f(x, x_1, \cdots, x_n),\ x,\ x_1,\ \cdots,\ x_n$$

を用いて定義したのであるが，これをもっと拡張して

$$f(0, x_1, \cdots, x_n), f(1, x_1, \cdots, x_n), \cdots, f(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n$$

全部を用いて定義することも考えられる。このような定義の方式を確定するために

$$\tilde{f}(y, x_1, \cdots, x_n)=\prod_{i<y} p_i{}^{f(i, x_1, \cdots, x_n)}$$

と定義すれば，f から $\tilde{f}$ は常に求まるが，逆にこの関係を満たす $\tilde{f}$ が存在すれば

$$f(i, x_1, \cdots, x_n)=(\tilde{f}(i+1, x_1, \cdots, x_n))_i$$

として求めることができる。この $\tilde{f}$ なる記号を用いれば，上に述べた定義の方式はつぎの形で与えられる。

$$\mathbf{II} \qquad f(y, x_1, \cdots, x_n)=g(y, \tilde{f}(y, x_1, \cdots, x_n), x_1, \cdots, x_n)$$

このような f がすべての g に対してただ一通りに定まることは，まず

$$\tilde{f}(y, x_1, \cdots, x_n)=\prod_{i<y} p_i^{g(i, \tilde{f}(i, x_1, \cdots, x_n), x_1, \cdots, x_n)}$$

から，$\tilde{f}$ を新しい記号であると思えば

$$\tilde{f}(0, x_1, \cdots, x_n)=1$$

$$\tilde{f}(i+1, x_1, \cdots, x_n)=\tilde{f}(i, x_1, \cdots, x_n)\cdot p_i^{g(i, \tilde{f}(i, x_1, \cdots, x_n), x_1, \cdots, x_n)}$$

となって，Ｉの定義にもどって $\tilde{f}$ が求められ，それから f を求めればよいから明らかである。

以上によって，つぎのことも明らかであろう。

1·2·37 g が原始帰納的関数で，f がⅡで与えられれば，f も原始帰納的関数である。

このⅡの形と場合に分ける方法とを組み合わせて，たとえば

$$\mathbf{II'} \quad f(x, x_1, \cdots, x_n)=\begin{cases} g_1(\tilde{f}(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n) \\ \qquad (Q_1(\tilde{f}(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n) \text{ が成立しているとき}) \\ g_m(\tilde{f}(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n) \\ \qquad (Q_m(\tilde{f}(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n) \text{ が成立しているとき}) \\ g_{m+1}(\tilde{f}(x, x_1, \cdots, x_n), x, x_1, \cdots, x_n) \\ \qquad (\text{それ以外のとき}) \end{cases}$$

という形の定義をすることもある。ここで，$Q_1, \cdots, Q_m$ は互いに相反する命題であるとする。もちろん，$g_1, \cdots, g_{m+1}, Q_1, \cdots, Q_m$ が原始帰納的関数であれば，f もやはり原始帰納的関数になるわけである。

今後，このような形を，多少の変形を含めたものも含めてⅡ′とよぶことにする。以下，2, 3 の例をあげよう。

例 1 f をつぎのもので定義する。

$$\begin{cases} f(0)=a \\ f(1)=b \\ f(x+2)=g(x, f(x), f(x+1)) \end{cases}$$

これは，つぎのように II′ の形と思ってよい。

$$f(x)=\begin{cases} a & (x=0 \text{ のとき}) \\ b & (x=1 \text{ のとき}) \\ g(x\dot{-}2, f(x\dot{-}2), f(x\dot{-}1)) & (\text{それ以外のとき}) \end{cases}$$

ここで，$f(x\dot{-}2)$，$f(x\dot{-}1)$ は $(\tilde{f}(x))_{x\dot{-}2}$，$(\tilde{f}(x))_{x\dot{-}1}$ と思うわけである。

例 2 f をつぎのもので定義する。

$$f(x)=\begin{cases} 0 & (x=0 \text{ のとき}) \\ g(x, f((x)_1), f((x)_2) & (x\neq 0 \text{ のとき}) \end{cases}$$

これは，つぎのように II′ の形式と思ってよい。

$$f(x)=\begin{cases} 0 & (x=0 \text{ のとき}) \\ g(x, (\tilde{f}(x))_{(x)_1}, (\tilde{f}(x))_{(x)_2}) & (\text{それ以外のとき}) \end{cases}$$

1・3 帰納的関数

われわれは，計算できる関数という直観的な概念をもっている。たとえば，これまで述べてきた原始帰納的な関数はすべて計算できる関数であるといってよいだろう。ところで，われわれの計算できる関数という直観的な概念が，原始帰納的な関数でちょうど表わされているであろうか。

この答がノーであることは，つぎのようにただちにわかる。いま，原始帰納的な関数は 1・2 節で述べた 1・2・1～1・2・5 で確実にかき並べることができる。したがって，原始帰納的関数を全部並べつくしてゆくことは，そうむずかしいことではない。これを f_0, f_1, f_2, $\cdots$ としよう。ここで，n が与えられれば，f_n がどのような関数であるかを正確に求められるようにしておかなければならない。ところで，f_0, f_1, f_2, $\cdots$ の中から 1 変数の関数の部分列をとり出して，それを f_0', f_1', f_2', $\cdots$ とすれば，やはり n を与えれば，われわれはいつでも f_n' を求めることができる。いま，$f'_{n-1}=f_k$ であるとして，f_{k+1}, f_{k+2}, $\cdots$

と調べてゆけば必ずいつか1変数の関数にゆきつくにちがいない(1変数の原始帰納的関数は無限にたくさんあり，それはすべて $f_0, f_1, \cdots$ の中にはいっているのであるから)。最初にぶつかったものを f_n' とすればよい。いま

$$g(x)=\overline{\mathrm{sg}}(f_x'(x))$$

とおけば，われわれは x が与えられれば f_x' を計算することができ，したがって $f_x'(x)$ を計算することができるから，これはわれわれの計算できる関数の直観を満たすものといってよいであろう。ところで，いま $g(x)$ が原始帰納的関数であるとすれば

$$g(x)=f_n'(x)$$

となる n が存在するにちがいない。したがって

$$g(n)=f_n'(n)$$

が得られる。

一方

$$g(n)=\overline{\mathrm{sg}}(f_n'(n))=\overline{\mathrm{sg}}(g(n))$$

となって矛盾する。

この例からもわかるように，われわれの計算できる関数という直観的な概念はかなり広い概念のように思われる。たとえば，1·2·1～1·2·5 に似たような新しい関数をつくる方法をつけ加えても，上の証明はそのまま成立する場合が多いように思われる。したがって，われわれの‘計算できる関数という直観的な概念’の数学的な定義を与えることは，あまり容易ではないように思われた。

A. Church は，これに関してつぎのような提言をした。これが **Church の thesis** とよばれるものである。

帰納的関数(recursive function)というものをつぎのように定義しよう。

1·2·1′～1·2·5′ を，1·2·1～1·2·5 の中の原始帰納的関数をすべて帰納的関数でおきかえたものとする。

1·2·1′～1·2·5′

このとき，帰納的な関数はつぎのように定義される。

1·3·1　g が帰納的関数で

$$\forall x_1, \cdots, x_n \exists y(g(x_1, \cdots, x_n, y)=0)$$

が成立しているときに

$$f(x_1, \cdots, x_n)=\mu y(g(x_1, \cdots, x_n, y)=0)$$

で定義される関数は帰納的関数である。

1·3·2　1·2·1′～1·2·5′と1·3·1で定義できる関数だけが帰納的関数である。

さて，Church の thesis とは，‘計算できる関数’の全体というものを帰納的な関数の全体として定義しようというものである。

現在までの数学の発展は，Church の thesis が正しいことを実証しているようであり，Church の thesis は現在は正しい提案としてほとんどすべての数学者に受け入れられているといっても過言ではないだろう(2, 3 の反対意見はないではない。しかし，そういう反対も，人をうなずかせる反例を提示しているわけではない。現在，こういう反対は異端と考えられている)。したがって，語の問題などで，effective な(計算できるという意味)解法がないという否定的命題を証明するためには，いつでも上に定義された帰納的な手法では問題が解けないということをいえば十分なのである。

さて，この帰納的関数の定義において，1·3·1 がわれわれの計算できるという概念をはみ出さないことを説明しよう。

すなわち，g は計算できる関数であって

$$\forall x_1, \cdots, x_n \exists y(g(x_1, \cdots, x_n, y)=0)$$

が成立しているものとする。いま

$$f(x_1, \cdots, x_n)=\mu y(g(x_1, \cdots, x_n, y)=0)$$

を，$x_1, \cdots, x_n$ が具体的に与えられたとして計算してゆくことを考えよう。

まず，$g(x_1, \cdots, x_n, 0)$ を計算してみる。答が 0 ならば $f(x_1, \cdots, x_n)=0$ となってメデタシメデタシである。もしそうでなければ $g(x_1, \cdots, x_n, 1)$ を計算してみる。もし答が 0 ならばメデタシメデタシである。もしそうでなければ $g(x_1, \cdots, x_n, 2)$ を計算してみる。こうやってメデタシメデタシになるまで $g(x_1, \cdots, x_n, k)$ の k をどこまでも計算してゆくわけである。ところで，この操作は必ず有限回で終了してメデタシメデタシというところがやってくること

に決まっていれば，確かに $f(x_1, \cdots, x_n)$ は計算できる関数である。この有限回で終了してしまうことに決まっているという条件が，ちょうど

$$\forall x_1, \cdots, x_n \exists y (g(x_1, \cdots, x_n, y)=0)$$

という条件になっているわけである。

さて，前と同様に，$P(x_1, \cdots, x_n)$ の特性関数が帰納的であるとき P が帰納的関数ということにすれば，1·2 節で述べた原始帰納的関数のいろいろな性質において，原始帰納的関数をすべて帰納的関数にかえたものがすべて成立することは明らかであろう。さらに，つぎの性質が成立する。

1·3·3　$x=f(x_1, \cdots, x_n)$ が帰納的命題ならば，f も帰納的関数である。

[証明]　$x=f(x_1, \cdots, x_n)$ を $P(x_1, \cdots, x_n, x)$ とすれば，P は帰納的命題である。いま，P の特性関数を g とすれば，g は帰納的関数である。ところで，f は関数であるから

$$\forall x_1, \cdots, x_n \exists y P(x_1, \cdots, x_n, y)$$

は成立している。すなわち

$$\forall x_1, \cdots, x_n \exists y (g(x_1, \cdots, x_n, y)=0)$$

は成立している。

一方，明らかに

$$f(x_1, \cdots, x_n)=\mu y (g(x_1, \cdots, x_n, y)=0)$$

であるから，f は帰納的関数である。

この証明の中から明らかなように，つぎの性質が成立する。

1·3·4　$P(x_1, \cdots, x_n, x)$ が帰納的関数で

$$\forall x_1, \cdots, x_n \exists y P(x_1, \cdots, x_n, y)$$

が成立すれば，$\mu y P(x_1, \cdots, x_n, y)$ は帰納的関数である。

さて，帰納的関数のもう少し詳しい性質にふれるためには，帰納的関数のもう1つ別の定義を考えなければならない。これをつぎの定理の形で述べることにする。

定理 1　いま，F をつぎのように定義された関数族であったとする。

1·3·5　$a+b$, $a \cdot b$ は F の関数である。さらに，$f_<$ を $<$ の特性関数とすれば，$f_<$ はFの関数である。また

$$f(x_1,\ \cdots,\ x_n)=x_i \qquad (1 \leq i \leq n)$$

とすれば，f はFの関数である。

1·3·6　g, h_1, $\cdots$, h_k が F の関数であるとき

$$f(x_1,\ \cdots,\ x_n)=g(h_1(x_1,\ \cdots,\ x_n),\ \cdots,\ h_k(x_1,\ \cdots,\ x_n))$$

とすれば，f はFの関数である。

1·3·7　g がFの関数であって

$$\forall x_1,\ \cdots,\ x_n \exists y(g(x_1,\ \cdots,\ x_n,\ y)=0)$$

が成立していれば

$$f(x_1,\ \cdots,\ x_n)=\mu y(g(x_1,\ \cdots,\ x_n,\ y)=0)$$

で定義された f も F の関数である。

1·3·8　F の関数は 1·3·5〜1·3·7 で定義されたものだけである。このとき，F と帰納的関数の全体の集合とは一致する。

[証明]　F の関数が帰納的であることは明らかであるから，逆だけを証明すればよい。そのために，まずいろいろな関数がFに属することをいうが，たいていは 1·2 節と大同小異であるから証明を省略する。ある命題がFに属するというのは，その特性関数がFに属することであるとする。

1·3·9　PがFに属していて

$$\forall x_1,\ \cdots,\ x_n \exists y P(x_1,\ \cdots,\ x_n,\ y)$$

ならば

$$\mu y P(x_1,\ \cdots,\ x_n,\ y)$$

も F に属する。

1·3·10　$f(x_1,\ \cdots,\ x_n)=k$ とすれば，$f \in F$ となる。

[証明]　$f(x_1,\ \cdots,\ x_n)=0$ ならば

$$f(x_1,\ \cdots,\ x_n)=\mu x(x=0)$$

であり，$f(x_1,\ \cdots,\ x_n)=k+1$ ならば

$$f(x_1,\ \cdots,\ x_n)=\mu x(k<x)$$

であるからよい。ここに，$x=0$ の x は $g(x_1, \cdots, x_n, x)=x$ なる関数と思えばよい。また，第2の $k<x$ は，$f_<$ がはいっているからよい。

1·3·11 $P, Q \in F$ ならば

$$\neg P,\ P \vee Q, P \wedge Q,\ P \to Q,\ P \leftrightarrow Q \in F$$

となる。

[証明] $\neg P$ の特性関数は $0<f(x_1, \cdots, x_n)$ の特性関数で（ここに，$f(x_1, \cdots, x_n)$ は P の特性関数とする），$f_<$ がはいっているから明らか。その他は 1·2 節と同じ。

1·3·12 $P \in F$ ならば

$\mu x<yP(x_1, \cdots, x_n, x)$, $\exists x<yP(x_1, \cdots, x_n, x)$, $\forall x<yP(x_1, \cdots, x_n, y)$

は，すべて F に属する。

[証明] $\mu x<yP(x_1, \cdots, x_n, x)=\mu x(x<y \wedge P(x_1, \cdots, x_n, x))$

あとは前と同じ。

1·3·13

$$a \dot{-} b \in F$$

[証明]

$$a \dot{-} b=\mu x(b+x=a \vee a<b)$$

1·3·14 $Q_1, \cdots, Q_m$ が F に属し，互いに相反するとする。f が $f_1, \cdots, f_{m+1}$ と $Q_1, \cdots, Q_m$ から場合に分けて定義して，$f_1, \cdots, f_{m+1} \in F$ ならば $f \in F$ である。

定理の証明のためには，以上により $g, h \in F$ のときⅠで定義される f が，また F に属することを証明すればよいことがわかる。これをいうために，$J(a, b)=c$ は

$$2c=(a+b)^2+3a+1$$

であるから，F にはいっていることに注意しておく。

1·3·15 いま，$a_0, \cdots, a_{n-1}$ を任意の有限列とするとき，ある b と c とが存在して

$$(b \equiv a_i \pmod{1+(i+1)c}) \wedge (a_i<1+(i+1)c)$$

がすべての $i<n$ に対して満たされているようにできる。ここで，c はいくらでも大きくすることができる。

[証明] $n!\mid c$ であるようにかってに c をとると，$i<j<n$ なる i, j と素数 p に対して

$$p\mid(1+(i+1)c)\land p\mid(1+(j+1)c)\to p\mid(j-i)c$$
$$\to p\mid c$$

となって矛盾するから

$$(1+(i+1)c,\ 1+(j+1)c)=1$$

である。ゆえに，剰余定理より

$$b\equiv a_i \qquad (\bmod 1+(i+1)c;\ i<n)$$

が成立するような b が存在する。

c はいくらでも大きくとれるから，$a_i<1+(i+1)c$ が成立するようにできる。

1·3·16 $\beta(a, i)=\mu x<(a\dot{-}1)\,\exists y<a\,\exists z<a(a=J(y, z))$
$\land(1+(i+1)z\mid(y-x)\land 1+(i+1)z\mid(x-y)$
$\land x<1+(i+1)z)$

とおけば，有限列 a_0, a_1, $\cdots$, a_{n-1} に対して，ある a が存在して

$$\beta(a, i)=a_i \qquad (i<n)$$

となる。

[証明] 1·3·15 より明らか。

最後に，f が g, h から 1·1 節の I で定義されていて，$g, h\in F$ ならば $f\in F$ であることを示すことにする。

β は明らかに F の関数であるから

$$\varphi(x, x_1, \cdots, x_n)$$
$$=\mu a(\beta(a, 0)=g(x_1, \cdots, x_n)$$
$$\land\forall i<x(\beta(a, i+1)=h(\beta(a, i), x, x_1, \cdots, x_n)))$$

とおけば，明らかに φ は F に属し

$$i\le x\to f(i, x_1, \cdots, x_n)=\beta(\varphi(x, x_1, \cdots, x_n), i)$$

となる。ゆえに

$$f(x, x_1, \cdots, x_n)=\beta(\varphi(x, x_1, \cdots, x_n), x)$$

となって，$f\in F$ なることがわかった。

1・4　帰納的可算について

ある命題 $P(x_1, \cdots, x_n)$ が帰納的可算(recursive enumerable)であるというのは，帰納的な命題 $Q(x_1, \cdots, x_n, y_1, \cdots, y_n)$ があって

$$P(x_1, \cdots, x_n) \leftrightarrow \exists y_1, \cdots, y_n Q(x_1, \cdots, x_n, y_1, \cdots, y_n)$$

とかけることである。

ここに

$$\exists y_1, \cdots, y_n Q(x_1, \cdots, x_n, y_1, \cdots, y_n)$$
$$\leftrightarrow \exists y Q(x_1, \cdots, x_n, (y)_1, \cdots, (y)_n)$$

であるから，帰納的可算をつぎのように定義しても同じである。

帰納的な命題 $Q(x_1, \cdots, x_n, y)$ があって

$$P(x_1, \cdots, x_n) \leftrightarrow \exists y Q(x_1, \cdots, x_n, y)$$

である。

もちろん，Pが帰納的ならば，Pは帰納的可算である。この逆が一般に成立しないことはあとで述べるが，これに関係したつぎの定理がある。

定理 1　Pと $\neg P$ がともに帰納的可算ならば，Pは帰納的である。

[証明]

$$P(x_1, \cdots, x_n) \leftrightarrow \exists y Q(x_1, \cdots, x_n, y)$$
$$\neg P(x_1, \cdots, x_n) \leftrightarrow \exists y R(x_1, \cdots, x_n, y)$$

であって，Q, R はともに帰納的であるとする。このとき

$$\forall x_1, \cdots, x_n (P(x_1, \cdots, x_n) \vee \neg P(x_1, \cdots, x_n))$$

が成立するから

$$\forall x_1, \cdots, x_n (\exists y Q(x_1, \cdots, x_n, y) \vee \exists y R(x_1, \cdots, x_n, y))$$

ゆえに

$$\forall x_1, \cdots, x_n \exists y (Q(x_1, \cdots, x_n, y) \vee R(x_1, \cdots, x_n, y))$$

となる。ゆえに，$Q \vee R$ は帰納的であるから

$$f(x_1, \cdots, x_n) = \mu y (Q(x_1, \cdots, x_n, y) \vee R(x_1, \cdots, x_n, y))$$

で f を定義すれば，f は帰納的で，つぎの条件

$$Q(x_1, \cdots, x_n, f(x_1, \cdots, x_n)) \vee R(x_1, \cdots, x_n, f(x_1, \cdots, x_n))$$

を満たす。

ところで

$$P(x_1, \cdots, x_n) \to \neg \exists y R(x_1, \cdots, x_n, y)$$

であるから

$$P(x_1, \cdots, x_n) \to \neg R(x_1, \cdots, x_n, f(x_1, \cdots, x_n))$$
$$\to Q(x_1, \cdots, x_n, f(x_1, \cdots, x_n))$$

となる。

逆に

$$Q(x_1, \cdots, x_n, f(x_1, \cdots, x_n)) \to \exists y Q(x_1, \cdots, x_n, y)$$

は明らかであるから

$$P(x_1, \cdots, x_n) \leftrightarrow Q(x_1, \cdots, x_n, f(x_1, \cdots, x_n))$$

となって，Pが帰納的であることがわかる。

さらに簡単な帰納的可算の性質として，つぎのものがある。

1·4·1　P, Q が帰納的可算であるならば

$$P \wedge Q, \quad P \vee Q, \quad \exists y P(x_1, \cdots, x_n, y)$$
$$\exists y < x P(x_1, \cdots, x_n, y), \qquad \forall y < x P(x_1, \cdots, x_n, y)$$

もすべて帰納的可算である。

[証明]　$P \wedge Q$, $P \vee Q$ が帰納的可算であることは，つぎの式から明らかであろう。

$$\exists z P_0(z) \wedge \exists z Q_0(z) \leftrightarrow \exists z_1 \exists z_2 (P_0(z_1) \wedge Q_0(z_2))$$
$$\exists z P_0(z) \vee \exists z Q_0(z) \leftrightarrow \exists z (P_0(z) \vee Q_0(z))$$

$\exists y P(x_1, \cdots, x_n, y)$ が帰納的可算になることは明らか。

$\exists y < x P(x_1, \cdots, x_n, y)$ が帰納的可算になることは，つぎの式から明らかであろう。

$$\exists y < x \exists z P_0(z, x) \leftrightarrow \exists y \exists z (y < x \wedge P_0(z, x))$$

$\exists y < x P(x_1, \cdots, x_n, y)$ が帰納的可算になることは， つぎの式と 1·2·26 による。

$$\forall y < x \exists z P_0(z, x) \leftrightarrow \exists z \forall y < x P_0((z)_y, y)$$

ここで注意すべきことは，P が帰納的可算であっても，$\neg P$，$\forall zP(z)$ が帰納的可算になるとはかぎらないことである。反例はあとで与えることにする。

さて，帰納的可算の定義は

$$\exists yP(x_1, \cdots, x_n, y)$$

で，Pが帰納的という形に表わされるということであったが，ここに帰納的という条件はいささか意味が複雑である。もう少し説明すれば，μx というようなえたいのしれないものがはいっている。μx がえたいのしれないものというのは，ちょっとわかりづらいかもしれないが，1·3·1 にはいっている条件

$$\forall x_1, \cdots, x_n \exists y(g(x_1, \cdots, x_n, y)=0)$$

は，あまりわかりよい条件ではない。帰納的関数の定義からこういう条件を除こうとすると，うまくゆかない。しかし，帰納的可算は帰納的よりはずっと広い命題のクラスなので，ある意味でいえばずっとおおざっぱである。逆にいえば，帰納的という性質はたいへんデリケートな性質である。したがって，帰納的可算の定義に帰納的を用いるのは，ある意味で不便である。したがって，これから証明してゆこうとすることは，帰納的可算が

$$\exists yP(x_1, \cdots, x_n, y)$$

なる形で ($P(x_1, \cdots, x_n, y)$ はもちろん帰納的である)，その中で非常に制限されたもっと具体的な特別な形をとってもよいということを証明することである。もちろん，この‘非常に制限されたもっと具体的な特別な形’というものはいろいろ考えられ，その応用の方面によってとり方が異なってくる。しかし，いずれも大同小異であると思ってさしつかえない。このところは少しばかり手間がかかるので，ゆっくり少しずつやってゆくことにする。

f と g とが，自然数を係数とする $x_1, \cdots, x_n$ の多項式であるとき

$$f(x_1, \cdots, x_n)=g(x_1, \cdots, x_n)$$

で表わされる命題をこの本では**初等的**ということにしよう（これは一般に通用する用語ではない）。

'初等的' に関する簡単な命題として，つぎのものがある。

1·4·2　P, Q が初等的な命題ならば

$$P \wedge Q, \qquad P \vee Q$$

も初等的である。

[証明]　P, Q は，それぞれ $f_1=g_1$, $f_2=g_2$ で定義されるとすれば

$$\begin{aligned} P \vee Q &\leftrightarrow f_1=g_1 \vee f_2=g_2 \\ &\leftrightarrow (f_1-g_1)(f_2-g_2)=0 \\ &\leftrightarrow f_1f_2+g_1g_2=f_1g_2+f_2g_1 \\ P \wedge Q &\leftrightarrow f_1=g_1 \wedge f_2=g_2 \\ &\leftrightarrow (f_1-g_1)^2+(f_2-g_2)^2=0 \\ &\leftrightarrow f_1{}^2+f_2{}^2+g_1{}^2+g_2{}^2=2f_1g_1+2f_2g_2 \end{aligned}$$

と表わすことができる。

1·4·3　$a=J(b, c)$ は初等的である。

[証明]　$$a=J(b, c) \leftrightarrow 2a=(b+c)^2+3b+c$$

1·4·4　$a \neq 0$, $a<b$, $a \neq b$, $a \equiv b \pmod c$, $a \mid b$ は明らかにつぎのように表わすことができる。

$$\begin{aligned} a \neq 0 &\leftrightarrow \exists x \leq a \ (a=x+1) \\ a<b &\leftrightarrow \exists z \leq b \ (b=a+z+1) \\ a \neq b &\leftrightarrow \exists x \leq a \, \exists y \leq b \ (b=a+y+1 \vee a=b+x+1) \\ a \equiv b \pmod c &\leftrightarrow \exists x \leq a \, \exists y \leq b \ (a=b+xc \vee b=a+yc) \\ a \mid b &\leftrightarrow \exists x \leq b \ (ax=b) \end{aligned}$$

ここに，右辺のカッコの中はすべて初等的であることに注意されたい。

さて，$P(x_1, \cdots, x_n)$ がつぎの形に表わされるとき，P を **diophantine** という。

$$\exists y(f(x_1, \cdots, x_n, y)=g(x_1, \cdots, x_n, y))$$

ここで，f と g はともに自然数を係数とする多項式であるとする。

さらに，$P(x_1, \cdots, x_n)$ がつぎの形で表わされるとき，P を**広い意味で di-**

ophantine とよぶことにする。

$$\exists y \forall k \leq y \exists z_1 \leq y \cdots \exists z_n \leq y Q(x_1, \cdots, x_n, y, k, z_1, \cdots, z_n)$$

ここに，Qは初等的であるとする。

Pが広い意味で diophantine であれば帰納的可算であることは明らかであるが，ここ当分の間の目的はこの逆であって，帰納的可算な命題は広い意味で diophantine であることを証明しようというものである。さらに第2章では，広い意味での diophantine は diophantine であることを証明する。さしあたって，$J: N \times N \to N$ は bijection であるから，$K: N \to N$, $L: N \to N$ で

$$J(K(a), L(a)) = a$$
$$K(J(a, b)) = a$$
$$L(J(a, b)) = b$$

を満たす K, L が存在する。明らかにつぎの式が成立する。

$$K(a) \leq a, \qquad L(a) \leq a$$

これらはよく，つぎのように用いられる。

1·4·5 $$\exists y \exists z \forall u A(u, y, z) \leftrightarrow \exists x \forall u A(u, K(x), L(x))$$
$$\leftrightarrow \exists x \forall u \exists y < x \exists z < x$$
$$(x = J(y, z) \wedge A(u, y, z))$$

1·4·6 P, Q を広い意味の diophantine とすれば，$P \wedge Q$ も広い意味の diophantine である。

［証明］ 簡単のために P, Q を1変数とする。

$$P(x) \leftrightarrow \exists y_1 \forall k_1 \leq y_1 \exists z_1{}^1 \leq y_1 \cdots \exists z_n{}^1 \leq y_1 P_0(x, y_1, k_1, z_1{}^1, \cdots, z_n{}^1)$$
$$Q(x) \leftrightarrow \exists y_2 \forall k_2 \leq y_2 \exists z_1{}^2 \leq y_2 \cdots \exists z_m{}^2 \leq y_2 Q_0(x, y_2, k_2, z_1{}^2, \cdots, z_m{}^2)$$

とすれば(ここに，P_0, Q_0 は初等的とする)，$P(x) \wedge Q(x)$ はつぎの命題と同等である。

$$\exists y_1 \exists y_2 \forall k_1 \leq y_1 \forall k_2 \leq y_2 \exists z_1{}^1 \leq y_1 \cdots \exists z_n{}^1 \leq y_1 \exists z_1{}^2 \leq y_2 \cdots \exists z_n{}^2 \leq y_2$$
$$(P_0(x, y_1, k_1, z_1{}^1, \cdots, z_2{}^1) \wedge Q_0(x, y_2, k_2, z_1{}^2, \cdots, z_n{}^2))$$

これはさらに

$$\exists y \forall k \leq y \exists z_1{}^1 \leq y \cdots \exists z_n{}^1 \leq y \exists z_1{}^2 \leq y \cdots$$

$$\exists z_n{}^2 \leq y \exists y_1 \leq y \exists y_2 \leq y \exists k_1 \leq y \exists k_2 \leq y$$
$$(P_0(x, y_1, k_1, z_1{}^1, \cdots, z_n{}^1) \land Q_0(x, y_2, k_2, z_1{}^2, \cdots, z_n{}^2)$$
$$\land k_1 \leq y_1 \land k_2 \leq y_2 \land z_1{}^1 \leq y_1 \land \cdots \land z_n{}^1 \leq y_1$$
$$\land z_1{}^2 \leq ky_2 \land \cdots \land z_m{}^2 \leq y_2 \land y = J(y_1, y_2) \land k = J(k_1, k_2))$$

ゆえに，命題は

$$s \leq y_i \leftrightarrow \exists u \leq y \ (y_i = s + u)$$

から明らかである。

1·4·7 $P(a_1, \cdots, a_m, a)$ が広い意味の diophantine とすれば，$\exists x P(a_1, \cdots, a_m, x)$ も広い意味の diophantine である。

[証明] 簡単のために，$m=1$ としてつぎの式が成立するものとする。

$$P(a, x) \leftrightarrow \exists y \forall k \leq y \exists z_1 \leq y \cdots \exists z_n \leq y P_0(a, x, y, k, z_1, \cdots, z_n)$$

ここで，P_0 は初等的とする。このとき，$\exists x P(a, x)$ は，つぎの命題

$$\exists y \forall k \leq y \exists z_1 \leq y \cdots \exists z_n \leq y \exists x \leq y \exists v \leq y$$
$$(J(x, v) = y \land k \leq v \land z_1 \leq v \land \cdots \land z_n \leq y$$
$$\land P_0(a, x, v, k, z_1, \cdots, z_n))$$

と同等である。

あとは 1·4·6 の証明と同じようにすればよい。

1·4·8 $\forall x < a \exists y \forall k \leq y A(x, y, k)$ は，つぎの命題と同等である。

$$\exists \tilde{y} \forall w \leq \tilde{y} \exists y \leq \tilde{y} \exists u \leq \tilde{y} \exists v \leq \tilde{y} \exists x \leq \tilde{y} \exists k \leq \tilde{y}$$
$$(\neg(w = J(x, k) \land k \leq y) \lor (\tilde{y} = J(u, v) \land (u \equiv y (\mathrm{mod}\, 1 + (x+1)v))$$
$$\land (y < 1 + (x+1)v) \land A(x, y, k))$$

[証明] 1·3·15 より明らかに，$\forall x < a \exists y \forall k \leq y A(x, y, k)$ は，つぎの命題と同等である。

$$\exists \tilde{y} \forall x < a \forall k \leq \tilde{y} \exists y \leq \tilde{y} \exists u \leq \tilde{y} \exists v \leq \tilde{y}$$
$$(k \leq y \rightarrow \tilde{y} = J(u, v) \land (u = y (\mathrm{mod}\, 1 + (x+1)v))$$
$$\land (y < 1 + (x+1)v) \land A(x, y, k))$$

ここで，このような $\tilde{y}$ をいくらでも大きくとることを考えれば，証明が完成する。

1·4·9　$P(a_1, \cdots, a_n, a)$ が広い意味の diophantine であれば，$\forall x<aP(a_1, \cdots, a_n, x)$ も広い意味の diophantine である。

[証明]　簡単のために，$P(a, x)$ の形で，それはつぎの形と同等とする。

$$\exists y \forall k \leq y \exists z \leq y P_0(a, x, y, k, z)$$

ここで，P_0 は初等的とする。

したがって，$\forall x<aP(b, x)$ はつぎのものと同等になる。

$$\forall x<a \exists y \forall k \leq y \exists z \leq y P_0(b, x, y, k, z)$$

ここに，1·4·8 を適用して，1·4·4 を用いればよい。

1·4·10　$f(a_1, \cdots, a_n)$ を帰納的関数とすれば，$f(a_1, \cdots, a_n)=b$ は広い意味で diophantine である。

[証明]　1·3 節の定理 1 における F で表わされた帰納的関数の定義によって，数学的帰納法を用いて証明する。

$$a_i=b, \quad a+b=c, \quad a \cdot b=c$$

については明らかである。$f_<$ については

$$f_<(a, b)=c \leftrightarrow (a<b \wedge c=0) \vee (b \leq a \wedge c=1)$$

から，1·4·4 により明らかである。つぎに

$$f(x_1, \cdots, x_n)=g(h_1(x_1, \cdots, x_n), \cdots, h_k(x_1, \cdots, x_n))$$

のときは

$$f(a_1, \cdots, a_n)=b \leftrightarrow \exists x_1, \cdots, x_n(b=g(x_1, \cdots, x_k) \\ \wedge x_1=h_1(a_1, \cdots, a_2) \wedge \cdots \wedge x_k=h_k(a_1, \cdots, a_n))$$

このあとは，1·4·6, 1·4·7 より明らかである。つぎに

$$f(x_1, \cdots, x_n)=\mu x(g(x_1, \cdots, x_n, x)=0)$$

のときは

$$f(a_1, \cdots, a_n)=b \leftrightarrow g(a_1, \cdots, a_n, b)=0 \\ \wedge \forall x<b(g(a_1, \cdots, a_n, x) \neq 0)$$

であるから

$$\forall x<b \exists y(g(a_1, \cdots, a_n, x)=y+1)$$

をいえばよい。ゆえに，1·4·7 と 1·4·9 とによって明らかである。

定理 2　帰納的可算な命題は広い意味の diophantine である。

[証明]　1・4・10 と 1・4・7 とにより明らかである。

1・5　ゲーデル数

ここで行なうことは，数理論理学できわめて広範囲に行なわれていることであるが，ここではごく特殊な場合にしか実行しない。

やりたいことは

$$\forall k \leq a \exists z_1 \leq a \cdots \exists z_n \leq a P(x_1, \cdots, x_n, a, k, z_1, \cdots, z_n)$$

で，P が初等的であるようなすべての命題にうまく自然数を対応させて，その対応が injection になるようにしようということである。この対応させられた自然数をこの命題のゲーデル数という。このゲーデル数をうまく対応させることを符号化(コーディング)ということもある。

A のゲーデル数を

$$\ulcorner A \urcorner$$

とかくことにする。最初にわれわれは変数の範囲を固定しないと困るから，変数を固定して

$$a_0, \ a_1, \ a_2, \ \cdots$$

だけしか用いないことにする。このゲーデル数を

$$\ulcorner a_i \urcorner = 2^{i+1}$$

と定義することにする。

$$\mathrm{Var}(x) \leftrightarrow \exists y (x = 2^{y+1})$$

で定義すれば，$\mathrm{Var}(x)$ ということは，x がある変数のゲーデル数になっているということ，すなわち $\ulcorner a_i \urcorner$ の形になっているということである。

さらに，われわれは 0 と 1 のゲーデル数をつぎのように定義することにする。

$$\ulcorner 0 \urcorner = 3, \qquad \ulcorner 1 \urcorner = 3^2$$

さらに，t_1, t_2 のゲーデル数が $\ulcorner t_1 \urcorner$, $\ulcorner t_2 \urcorner$ であるとき

$$\ulcorner t_1 + t_2 \urcorner = 5 \cdot 2^{\ulcorner t_1 \urcorner} \cdot 3^{\ulcorner t_2 \urcorner}$$

$$\ulcorner t_1 \cdot t_2 \urcorner = 7 \cdot 2^{\ulcorner t_1 \urcorner} \cdot 3^{\ulcorner t_2 \urcorner}$$

によって「t_1+t_2」，「$t_1 \cdot t_2$」を定義することにする。

いま，pol(x) という関数をつぎのように定義する。

pol(x)=0　（x が 2^{i+1} の形か 3 か 3^2 のとき）

pol(x)=0　（x が $5 \cdot 2^y \cdot 3^z$ の形で，pol(y)=pol(z)=0 のとき）

pol(x)=0　（x が $7 \cdot 2^y \cdot 3^z$ の形で，pol(y)=pol(z)=0 のとき）

pol(x)=1　（上のどの場合でもないとき）

この関数は，明らかに場合に分ける定義と，1・2 節，II の定義の仕方とを組み合わせたものであるから，pol は原始帰納的関数である。

いま，Pol(x) を

$$\mathrm{Pol}(x) \leftrightarrow \mathrm{pol}(x)=0$$

と定義すれば，Pol(x) が成立するということは，x がある多項式のゲーデル数になっていることを意味する。

上の定義によれば，自然数を表わすものはわれわれの形式言語の中では

$$0,\ 1,\ 1+1,\ (1+1)+1,\ ((1+1)+1)+1,\ \cdots$$

であると考えてよい。これを数字(numeral)とよんで

$$n_0,\ n_1,\ n_2,\ n_3,\ \cdots$$

とかくことにする。「n_i」に相当するものを i の関数と思って定義して，これを $n(i)$ とおけば

$$n(0)=3$$

$$n(1)=3^2$$

$$n(i+1)=5 \cdot 3^{n(i)} \cdot 3^{3^2} \qquad (i \neq 0 \text{ のとき})$$

となるから，明らかに $n(i)$ は原始帰納的関数である。

Nl(x) を，x がある数字のゲーデル数になっていることと定義すれば

$$\mathrm{Nl}(x) \leftrightarrow \exists i < x\ (x=n(i))$$

であるから，Nl は原始帰納的命題である。

いま，$f(a_0, \cdots, a_n)$ は多項式であるとする。この a_i のところに数字 n を代入してできる $f(a_0, \cdots, a_{i-1}, n, a_{i+1}, \cdots, a_n)$ を求めたとする。このとき

$$\ulcorner f(a_0, \cdots, a_n)\urcorner, \quad \ulcorner a_i\urcorner, \quad \ulcorner n\urcorner$$

から

$$f(a_0, \cdots, a_{i-1}, n, a_{i+1}, \cdots, a_n)$$

を求める方法を計算してみよう。

$$x=\ulcorner f(a_0, \cdots, a_n)\urcorner, \quad b=\ulcorner a_i\urcorner, \quad c=\ulcorner n\urcorner$$

とおけば，数字 c を多項式 $f(a_0, \cdots, a_n)$ の変数 a_i に代入するという意味で

$$\mathrm{plsub}\left(\binom{b}{c}x\right)$$

という3変数の関数を定義するわけである。これは，1·2 節で導入された記号 $(x)_i$ を用いれば，つぎの式で定義される。

$$\mathrm{plsub}\left(\binom{b}{c}x\right)=5\cdot 2^{\mathrm{plsub}\left(\binom{b}{c}(x)_0\right)}\cdot 3^{\mathrm{plsub}\left(\binom{b}{c}(x)_1\right)}$$ (Pol(x), Var(b), Nl(c) で $x=5\cdot 2^{(x)_0}\cdot 3^{(x)_1}$ の形のとき)

$$\mathrm{plsub}\left(\binom{b}{c}x\right)=7\cdot 2^{\mathrm{plsub}\left(\binom{b}{c}(x)_0\right)}\cdot 3^{\mathrm{plsub}\left(\binom{b}{c}(x)_1\right)}$$ (Pol(x), Var(b), Nl(c) で $x=7\cdot 2^{(x)_0}\cdot 3^{(x)_1}$ の形のとき)

$$\mathrm{plsub}\left(\binom{b}{c}x\right)=x$$ (Var(b), Nl(c) で Nl(x) のとき)

$$\mathrm{plsub}\left(\binom{b}{c}x\right)=x$$ (Var(b), Var(x), Nl(c) で $x\neq b$ のとき)

$$\mathrm{plsub}\left(\binom{b}{c}x\right)=c$$ (Var(x), Var(b), Nl(c) で $x=b$ のとき)

$$\mathrm{plsub}\left(\binom{b}{c}x\right)=0$$ (以上のいずれでもないとき)

この定義が 1·2 節, II′ になっていることは明らかであるから，$\mathrm{plsub}\left(\binom{b}{c}x\right)$ は原始帰納的関数である。

さらに多項式 $f(a_0, \cdots, a_n)$ が与えられたとき，この多項式の中に a_i が実際に現われるということを $\ulcorner f(a_0, \cdots, a_n)\urcorner$, $\ulcorner a_i\urcorner$ の関係として定義しよう。

まず，$x=\ulcorner f(a_0, \cdots, a_n)\urcorner$, $b=\ulcorner a_i\urcorner$ とおいて，この関係が成立するとき 0, そうでないとき 1 という関数を

$$\mathrm{varpl}(b, x)$$

と表わせば

$$\mathrm{varpl}(b, x)=\mathrm{varpl}(b, (x)_0)\cdot\mathrm{varpl}(b, (x)_1) \quad (\mathrm{Var}(b), \mathrm{Pol}(x) \text{ で } x=5\cdot2^{(x)_0}\cdot3^{(x)_1} \text{ または } x=7\cdot2^{(x)_0}\cdot3^{(x)_1} \text{ のとき})$$

$$\mathrm{varpl}(b, x)=0 \quad (\mathrm{Var}(b), \mathrm{Var}(x) \text{ で } b=x \text{ のとき})$$

$$\mathrm{varpl}(b, x)=1 \quad (\text{上のいずれでもないとき})$$

が成り立つ。この定義はやはり 1·2 節の II′ の形であるから，varpl(b, x) は原始帰納的関数である。したがって，上の関係は varpl$(b, x)=0$ であるから，やはり原始帰納的関数である。これをつぎのように表わすことにしよう。

$$\mathrm{Varpl}(b, x)$$

つぎに，初等的な命題

$$f(a_0, \cdots, a_n)=g(a_0, \cdots, a_n)$$

のゲーデル数を

$$11\cdot2^{\ulcorner f(a_0,\cdots,a_n)\urcorner}\cdot3^{\ulcorner g(a_0,\cdots,a_n)\urcorner}$$

によって定義しよう。この定義から，‘x がある初等的な命題のゲーデル数である’という命題を

$$\mathrm{Atom}(x)$$

で表わせば

$$\mathrm{Atom}(x)\leftrightarrow x=11\cdot2^{(x)_0}\cdot3^{(x)_1}\wedge\mathrm{Pol}((x)_0)\wedge\mathrm{Pol}((x)_1)$$

と表わされる。したがって，Atom(x) は原始帰納的命題である。ここに，Atom は atomic formula の略である。

x が初等的命題のゲーデル数，b が変数のゲーデル数 $\ulcorner a_i\urcorner$，c が数字のゲーデル数 $\ulcorner n\urcorner$ であるとするとき，この x の表わす初等的命題の a_i に n を代入し

てできる初等的命題のゲーデル数を x, b, c で表わすことを考えよう。これを

$$\mathrm{atsub}\left(\binom{b}{c}x\right)$$

とかくことにすれば

$$\mathrm{atsub}\left(\binom{b}{c}x\right)=11\cdot 2^{\mathrm{plsub}\left(\binom{b}{c}(x)_0\right)}\cdot 3^{\mathrm{plsub}\left(\binom{b}{c}(x)_1\right)}$$　（Atom(x), Var(b), Nl(c) のとき）

$$\mathrm{atsub}\left(\binom{b}{c}x\right)=0$$　（上の場合でないとき）

となるから，$\mathrm{atsub}\left(\binom{b}{c}x\right)$ もやはり原始帰納的関数である。

つぎに

$$x=\ulcorner f(a_0,\ \cdots,\ a_n)=g(a_0,\ \cdots,\ a_n)\urcorner,\qquad b=\ulcorner a_i\urcorner$$

とするとき，i が $f(a_0,\ \cdots,\ a_n)=g(a_0,\ \cdots,\ a_n)$ の中に実際に現われるという関係を x と b とで表わすことを考えよう。この関係を

$$\mathrm{Varat}(b,\ x)$$

と表わせば

$$\mathrm{Varat}(b,\ x)\leftrightarrow \mathrm{Atom}(x)\wedge(\mathrm{Varpl}(b,\ (x)_0)\vee \mathrm{Varpl}(b,\ (x)_1))$$

となるから，やはり Varat(b, x) は原始帰納的命題である。

さて，いよいよわれわれが求める，つぎのような二通りの形の命題のゲーデル数を考えることにしよう。

$$\forall a_1\leq a_0\,\exists a_{i_0}\leq a_0\cdots\,\exists a_{i_n}\leq a_0 P(a_0,\ a_1,\ a_2,\ a_{i_1},\ \cdots,\ a_{i_n})$$

$$\forall a_1\leq m\,\exists a_{i_0}\leq m\cdots\,\exists a_{i_n}\leq m P(a_1,\ a_2,\ a_{i_1},\ \cdots,\ a_{i_n})$$

ここに，P は初等的な命題で，m は数字であるとする。われわれは便宜上，a_{i_1}, $\cdots$, a_{i_n} の中に a_0, a_1, a_2 ははいっていないものとする。このとき，そのゲーデル数をそれぞれ

$$13\cdot 2^{\ulcorner m\urcorner}\cdot 3^{2^{\ulcorner a_{i_0}\urcorner}\cdot 3^{\ulcorner a_{i_1}\urcorner}\cdots p_n^{\ulcorner a_{i_n}\urcorner}}\cdot 5^{\ulcorner P(a_0,a_1,\cdots,a_{i_n})\urcorner}$$

または

$$13\cdot 2^{\ulcorner a_0\urcorner}\cdot 3^{2^{\ulcorner a_{i_0}\urcorner}\cdot 3^{\ulcorner a_{i_1}\urcorner}\cdots p_n^{\ulcorner a_{i_n}\urcorner}}\cdot 5^{\ulcorner P(a_0,a_1,\cdots,a_{i_n})\urcorner}$$

とおくことにする。

このとき，x がこのような形の命題のゲーデル数であるということを

$$\mathrm{Form}(x)$$

とおけば(formula からとった)，Form(x) はつぎの式で定義される。

$$x=13\cdot 2^{(x)_0}\cdot 3^{(x)_1}\cdot 5^{(x)_2}\wedge(\mathrm{Nl}((x)_0)\vee(x)_0=2)$$
$$\wedge\forall k<\mathrm{lh}((x)_1)(\mathrm{Var}((x)_{1k})\wedge(x)_{1k}\neq 2\wedge(x)_{1k}\neq 2^2\wedge(x)_{1k}=2^3)$$
$$\wedge\forall i,\ k<\mathrm{lh}((x)_1)(i\neq k\rightarrow(x)_{1i}\neq(x)_{1k})\wedge\mathrm{Atom}((x)_3)$$

したがって，Form(x) も原始帰納的命題である。

ある形式言語における表現が **closed** であるというのは，その表現の中に変数が1つもはいっていないか，またはその変数がすべて束縛されていることをいう。以下に，多項式が closed である，初等的命題が closed である，formula が closed である，という性質をその表現のゲーデル数についての性質で表わすことにしよう。

まず，‘x が closed な多項式のゲーデル数である’ ということを

$$\mathrm{Clpl}(x)$$

と表わすことにすれば

$$\mathrm{Clpl}(x)\leftrightarrow\mathrm{Pol}(x)\wedge\forall b<x(\mathrm{Var}(b)\rightarrow\neg\mathrm{Varpl}(b,x))$$

であるから，Clpl(x) は原始帰納的命題である。

つぎに，‘x が closed な初等的命題のゲーデル数である’ ということを

$$\mathrm{Clat}(x)$$

と表わすことにすれば

$$\mathrm{Clat}(x)\leftrightarrow\mathrm{Atom}(x)\wedge\mathrm{Clpl}((x)_0)\wedge\mathrm{Clpl}((x)_1)$$

となるから，Clat(x) も原始帰納的命題である。

つぎに，‘x が closed な formula のゲーデル数である’ ということを

$$\mathrm{Clfm}(x)$$

と表わすことにすれば，つぎのようになる。

$$\mathrm{Clfm}(x)\leftrightarrow\mathrm{Form}(x)\wedge\mathrm{Nl}((x)_0)\wedge\forall b<x(\mathrm{Varat}(b,(x)_2)$$

$$\rightarrow b=2^2 \vee \exists i<\mathrm{lh}((x)_1)(b=(x)_{1i}))$$

さて，x が formula のゲーデル数であるとき，その中の a_0 に n を代入するということを表わすことを考えよう。いま，$c=\ulcorner n\urcorner$ とするとき，この代入によってできたものを

$$\mathrm{fmsub}((2/c), x)$$

とかいて，これをつぎのように場合に分けて定義する。

$\mathrm{Form}(x)\wedge \mathrm{Nl}(c)\wedge \mathrm{Nl}((x)_0)$ のとき

$$\mathrm{fmsub}((2/c), x)=13\cdot 2^{(x)_0}\cdot 3^{(x)_1}\cdot 5^{\mathrm{plsub}((2/c),(x)_2)}$$

$\mathrm{Form}(x)\wedge \mathrm{Nl}(c)\wedge (x)_0=2$ のとき

$$\mathrm{fmsub}((2/c), x)=13\cdot 2^{c}\cdot 3^{(x)_1}\cdot 5^{\mathrm{plsub}((2/c),(x)_2)}$$

以上のいずれでもないとき

$$\mathrm{fmsub}((2/c), x)=0$$

もちろん，$\mathrm{fmsub}((2/c), x)$ なる形は原始帰納的関数である。

つぎに，x が formula のゲーデル数であるとき，その中の a_1 または a_2 に n を代入するということを表わすことを考えよう。$c=\ulcorner n\urcorner$ として，この代入によってできたものをそれぞれ

$$\mathrm{fmsub}(4, c;\ x), \qquad \mathrm{fmsub}(8, c;\ x)$$

によって表わせば

$\mathrm{Form}(x)\wedge \mathrm{Nl}(c)$ のとき

$$\mathrm{fmsub}(4, c;\ x)=13\cdot 2^{(x)_0}\cdot 3^{(x)_1}\cdot 5^{\mathrm{plsub}(\binom{4}{c}(x)_2)}$$

上の場合でないとき

$$\mathrm{fmsub}(4, c;\ x)=0$$

$\mathrm{Form}(x)\wedge \mathrm{Nl}(c)$ のとき

$$\mathrm{fmsub}(8, c;\ x)=13\cdot 2^{(x)_0}\cdot 3^{(x)_1}\cdot 5^{\mathrm{plsub}(\binom{8}{c}(x)_2)}$$

上の場合でないとき

$$\mathrm{fmsub}(8, c;\ x)=0$$

もちろん，$\mathrm{fmsub}(4, c;\ x)$ や $\mathrm{fmsub}(8, c;\ x)$ は原始帰納的関数である。

つぎに，変数の列 $a_{i_0}, \cdots, a_{i_k}$ が与えられたとき，これに数字の列 $n_0, \cdots, n_k$ をある formula の中で代入するという操作を定義しよう。

いま，この formula のゲーデル数を x, $2^{\ulcorner a_{i_0} \urcorner} \cdots p_k{}^{\ulcorner a_{i_k} \urcorner}$ を y, $c=2^{n_0} \cdots 3^{n_k}$ としたとき，もう少し一般に，つぎのように定義する。

$$\mathrm{fmsub}\left(0, \binom{y}{c}x\right)=13\cdot 2^{(x)_0}\cdot 3^{(x)_1}\cdot 5^{\mathrm{plsub}\left(\binom{(y)_0}{n((c)_0)}(x)_2\right)}$$

$$\mathrm{fmsub}\left(i+1, \binom{y}{c}x\right)=13\cdot 2^{(x)_0}\cdot 3^{(x)_1}\cdot 5^{\mathrm{plsub}\left(\binom{(y)_{i+1}}{n((c)_{i+1})}(z)_2\right)}$$

ここに，z は $\mathrm{fmsub}\left(i, \binom{y}{c}x\right)$ とおくことにする。

最後に，$\mathrm{fmsub}\left(\binom{y}{c}x\right)$ を

$$\mathrm{fmsub}\left(\binom{y}{c}x\right)=\mathrm{fmsub}\left(\mathrm{lh}(y), \binom{y}{c}x\right)$$

によって定義する。もちろん，この式は y と c とがちょうどピッタリとした条件を満たしているときにのみ意味をもってくる。もちろん，この関数も原始帰納的関数である。

1·6 truth definition

ここで行なうことも，数理論理学では広範囲に用いられることであるが，ここではごくかぎられた場合に，ごくかぎられた方法でやろうというわけである。

まず最初に，f が closed な多項式であるとする。すなわち，f には変数が1つもはいっていない。したがって，f の値を計算することができるわけである。その計算をしてできた答を，$\ulcorner f \urcorner$ から求める方法を求めようというわけである。いま，$x=\ulcorner f \urcorner$ とおいて，その求める値を $\mathrm{Val}(x)$ とおくことにする。ここに，Val は valuation からとったものである。これは場合に分けて，つぎのように定義できる。

$\mathrm{Clat}(x)$ でないとき

$$\mathrm{Val}(x)=0$$

とおく。

$\mathrm{Clat}(x)$ のときは，さらにつぎのように場合を分ける。

$$x=3 \quad \text{のときは} \qquad \mathrm{Val}(x)=0$$
$$x=3^2 \quad \text{のときは} \qquad \mathrm{Val}(x)=1$$

以上でないときは，さらにつぎのように分ける。

$$x=5\cdot 2^{(x)_0}\cdot 3^{(x)_1} \text{ のときは} \qquad \mathrm{Val}(x)=\mathrm{Val}((x)_0)+\mathrm{Val}((x)_1)$$
$$x=7\cdot 2^{(x)_0}\cdot 3^{(x)_1} \text{ のときは} \qquad \mathrm{Val}(x)=\mathrm{Val}((x)_0)\cdot\mathrm{Val}((x)_1)$$

この関数が原始帰納的関数であって，これが求めるものであることは明らかであろう。

つぎに，x が closed な初等的命題 $f=g$ のゲーデル数であったとき，この真偽は f の値と g の値とを計算して，それが等しいかどうかで決まるわけである。この真偽を「$f=g$」すなわち x から決定するにはどうしたらよいであろうか。これを

$$\mathrm{Trat}(x)$$

とおくことにする。ここに，Tr は truth からとったのである。Trat(x) は，つぎのように定義される。

$$\mathrm{Trat}(x) \leftrightarrow \mathrm{Clat}(x) \wedge \mathrm{Val}((x)_0)=\mathrm{Val}((x)_1)$$

この関係が求めるものであって，原始帰納的命題であることは明らかであろう。

x が closed formula A のゲーデル数であったとする。さらに，A の束縛変数のところをとり去った初等的命題の部分は a_1 を含んでいないものとする(この部分が a_0, a_2 を含んでいないことは closed の条件から出てくる)。このとき，A の真偽を「A」すなわち x から決定することを考えよう。このために，まず

$$l(i, n)$$

なる原始帰納的な関数をつぎのように定義する。

$$l(0, m)=1$$
$$l(i+1, m)=l(i, m)\cdot p_i^m$$

すなわち，$l(n, m)$ は

$$2^m\cdot 3^m \cdots p_{n-1}^m$$

を意味するわけである。

この上で，上の命題を $\mathrm{Tr'fm}(x)$ とおけば

$$\mathrm{Tr'fm}(x) \leftrightarrow \mathrm{Clfm}(x) \wedge \neg \mathrm{Varpl}(4, (x)_2)$$
$$\wedge \forall c \leq l(\mathrm{lh}((x)_1), (x)_0)\mathrm{Trat}\left(\mathrm{fmsub}\binom{(x)_1}{c}(x)_2\right)$$

これはもちろん原始帰納的命題であって，求めるものである。

最後に，x が closed formula のゲーデル数であるとき，この formula の真偽を，そのゲーデル数 x から決定することを考えよう。これを

$$\mathrm{Tr}(x)$$

とおくことにすれば，明らかに

$$\mathrm{Tr}(x) \leftrightarrow \mathrm{Clfm}(x) \wedge \forall k < (x)_0 \mathrm{Tr'fm}(\mathrm{Sub}(4, n(k)\,;\, x))$$

となる。したがって，Tr は原始帰納的命題である。

いま，任意の a_2 についての帰納的可算な命題 $A(a_2)$ をつぎの形で表わそう。

$$\exists a_0 \forall a_1 \leq a_0 \exists a_{i_1} \leq a_0 \cdots \exists a_{i_n} \leq a_0 P(a_0, a_1, a_2, a_{i_1}, \cdots, a_{i_n})$$

ここで，$a_{i_1}, \cdots, a_{i_n}$ は互いに相異なり，a_0, a_1, a_2 ではないものとし，Pは初等的命題とする。このとき

$$\forall a_1 \leq a_0 \exists a_{i_1} \leq a_0 \cdots \exists a_{i_n} \leq a_0 P(a_0, a_1, a_2, a_{i_1}, \cdots, a_{i_n})$$

のゲーデル数を e とおくことにする。すなわち

$$e = \ulcorner \forall a_1 \leq a_0 \exists a_{i_1} \leq a_0 \cdots \exists a_{i_n} \leq a_0 P(a_0, a_1, a_2, a_{i_1}, \cdots, a_{i_n}) \urcorner$$

このとき，$A(k)$ は明らかにつぎの命題と同等である。

$$\exists b \mathrm{Tr}(\mathrm{Sub}(2, n(b), \mathrm{Sub}(4, n(k), e)))$$

いま，$\mathrm{Tr}(\mathrm{Sub}(2, n(b), \mathrm{Sub}(4, n(k), e)))$ を

$$T(e, k, b)$$

とおけば，T はもちろん原始帰納的命題であって

$$A(k) \leftrightarrow \exists x T(e, k, x)$$

となる。すなわち，つぎの定理を得る。

定理 1　ある原始帰納的な命題 T が存在して，すべての a についての帰納的

可算な命題 $A(a)$ に対して，ある自然数 e が存在して

$$\forall a(A(a) \leftrightarrow \exists x T(e, a, x)$$

が存在する。

この定理で，T が原始帰納的命題であることと，T が A と無関係に定まることが重要である。もちろん，e は A によって定まる。しばしば，e のことを帰納的可算な命題 A のゲーデル数とよぶ。しかし，これはしばしば誤解のもととなる。

$$\exists a_0 \forall a_1 \leq a_0 \exists a_{i_1} \leq a_0 \cdots \exists a_{i_n} \leq a_0 P(a_0, a_{i_1}, \cdots, a_{i_n})$$

の形に対しては，ゲーデル数はただ1つにかぎられるが，$A(a)$ を与えたとき $A(a)$ と同等になる，このような形は無数に存在する。したがって，$A(a)$ に対応するゲーデル数は無数にあることになる。

また $\exists x T(e, a, x)$ は，T が原始帰納的命題であるから帰納的可算である。したがって，この定理は帰納的可算な命題をすべて並べつくすうまい帰納的可算な命題をみつけたことになっている。この T のことを，しばしば Kleene の T という。Kleene が最初に用い始めたからである。

定理 2　帰納的可算な命題で帰納的でないものが存在する。

[証明]　いま，すべての帰納的可算な命題が帰納的であるとすれば

$$\exists x T(a, a, x)$$

も帰納的である。したがって，つぎの命題も帰納的である。

$$\forall x \neg T(a, a, x)$$

帰納的な命題は帰納的可算であるから，ある e が存在して

$$\exists x T(e, a, x) \leftrightarrow \forall x \neg T(a, a, x)$$

が存在する。いま，この a に e を代入すれば

$$\exists x T(e, e, x) \leftrightarrow \forall x \neg T(e, e, x)$$

となって矛盾する。

1·7　決定問題への応用

1·5 節でわれわれは，特別な命題に対して特別なゲーデル数を対応させる方

法を考えた。

しかし，ゲーデル数を一般の言語に，もっと一般的な方法で対応させることができる。1つの方法は，その中に出てくるすべての記号に数字を対応させ，たとえば

	a_0,	a_1,	a_2,	$\cdots$							
には	2,	4,	8,	16, $\cdots$							
	=,	+,	·,	(,),	<,	∀,	∃,	∧,	¬,	∨	
にそれぞれ	3	5	7	9　11	13	15	17	19	21	22	

というようにして，formula を記号の列と考えて，それを

$$a_0,\ a_1,\ \cdots,\ a_n$$

とすれば，この列に

$$2^{\ulcorner a_0 \urcorner},\ 3^{\ulcorner a_1 \urcorner},\ \cdots,\ P_n{}^{\ulcorner a_n \urcorner}$$

を対応させるという方法である。このような方法によってもゲーデル数を対応させて，1·5 節で行なったのと類似の方法でいろいろな概念を定義し，必要な性質を証明することができる。

とにかく，いまわれわれが考える言語に，うまいゲーデル数の対応がつけられているものとして，そこである命題の列を

$$P_0,\ P_1,\ P_2,\ \cdots$$

とする。これは

$$\ulcorner P_0 \urcorner,\ \ulcorner P_1 \urcorner,\ \ulcorner P_2 \urcorner,\ \cdots$$

の大きさの順序に並んでいるものと思ってもよいし，何か別の方法であると思ってもよいが，とにかく

$$\ulcorner P_n \urcorner = f(n)$$

とおけば，f は帰納的な関数であるとする(具体的な例では，すべて原始帰納的である)。

このとき，P_0, P_1, P_2, $\cdots$ の決定問題を解けというのは，P_i が真か偽かを決定する方法をみいだせということである。P_i が真であるときは真で，偽であるときは偽というような決定方法では困るので，たいていは effective に決

定する方法をみいだせというようにいう。その意味は，P_i が具体的に与えられたとき，実際に**有限回**で確実に判定できるような方法をみいだせということである。

もう少し詳しくいうと，計算のできる関数 g をみいだして

$$g(\ulcorner P_i \urcorner)=0 \quad \text{ならば} \quad P_i \text{ が真}$$

で

$$g(\ulcorner P_i \urcorner)=1 \quad \text{ならば} \quad P_i \text{ が偽}$$

になるようにせよということである。

このように，問題の定式化が確定すると，今度は問題を否定的に解くことができるようになってくる。

たとえば，いま $P(a)$ という命題が与えられて，任意な数字 n に対して，$P(n)$ は上の $P_0, P_1, \cdots$ の1つであるとする。このとき

$$\ulcorner P(n) \urcorner = h(n)$$

とすれば，h は帰納的であるものとする(具体的にはたいてい原始帰納的である)。

いま，$P(a)$ が帰納的可算ではあるが，帰納的ではない命題とする。このとき，もし

$$g(\ulcorner P_i \urcorner)=0 \leftrightarrow \text{‘}P_i \text{ が真である’}$$

という帰納的な関数 g が存在したとすると

$$P(n) \leftrightarrow g(\ulcorner P(n) \urcorner)=0$$
$$\leftrightarrow g(h(n))=0$$

となる。

ところで，g, h は帰納的であるから，$g(h(n))=0$ は n の命題として帰納的である。ところが，$P(n)$ は n の命題として帰納的ではないから矛盾する。

以下，第2章，第3章でわれわれが行なうことは，すべて帰納的可算な命題 $A(a)$ に対して，上手に $P(a)$ を選べば，P は上の条件を満たし，さらに

$$A(a) \leftrightarrow P(a)$$

になることを証明して，決定問題が effective に解けないことを証明するのである。

第 2 章

ヒルベルトの第 10 問題

2・1　第 10 問題

ヒルベルトの第 10 問題とは，つぎの問題である。

いま

$$P(x_1, \cdots, x_n)$$

を，有理整数を係数とする $x_1, \cdots, x_n$ の多項式とするとき

$$P(x_1, \cdots, x_n)=0$$

が有理整数の根 $x_1, \cdots, x_n$ をもつかどうかを，effective に判定する方法を求めよ。

いま，ここに $x_1, \cdots, x_n$ の範囲を有理整数としたが，その範囲を自然数としても問題が同等の問題にしかかわらないことは，つぎのようにわかる。いま，有理整数の範囲で根が存在することを決定する方法が知られていたとして，自然数の範囲で根が存在することを決定したいと思えば，新しい変数

$$p_1,\ q_1,\ r_1,\ s_1,\ \cdots,\ p_n,\ q_n,\ r_n,\ s_n$$

を導入して

$$P(p_1{}^2+q_1{}^2+r_1{}^2+s_1{}^2, \cdots, p_n{}^2+q_n{}^2+r_n{}^2+s_n{}^2)=0$$

が有理整数の範囲で根をもつかどうかを調べてみればよい。ここに，任意の自然数は 4 個の平方数の和で表わされるというラグランジュの定理(高木貞治：初等整数論 71 ページ参照)を用いたのである。

逆に，いま自然数の範囲での根の存在の決定方法が与えられているとして，有理整数の範囲での根の存在を決定するには

$$P(x_1, \cdots, x_n)=0,\ P(-x_1, x_2, \cdots, x_n)=0,\ \cdots,\ P(-x_1, \cdots, -x_n)=0$$

なる 2^n 個の多項式について，自然数の範囲で根が存在するかどうかを調べてみればよい。

今後この章では，変数の範囲は常に自然数であるものとする。

さて，ヒルベルトの問題の目的は実際に effective な方法をみつけることにあったようであるが，この問題は M. Davis, H. Putnam, J. Robinson の結果を用いて Ju. v. Matijasevič によって否定的に解決されたので，ここに述べるのはその否定的な解決である。

$P(x_1, \cdots, x_n)=0$ に根が存在するという命題は

$$\exists x_1, \cdots, x_n\ (P(x_1, \cdots, x_n)=0)$$

で表わされるから，われわれは一般に

$$\exists x_1, \cdots, x_n\ (P(x_1, \cdots, x_n, y_1, \cdots, y_n)=0)$$

なる命題を考え，この形で表わされる命題を（$y_1, \cdots, y_n$ についての）diophantine な命題であるという。

われわれの最終目的は，つぎの定理である。

定理 1　すべての帰納的可算な命題は diophantine である。

この定理から，ヒルベルトの第 10 問題が否定的に解決されることは，1･7 節ですでに述べたところである。以下に，diophantine の性質をいろいろと調べていって，この定理を証明することにする。

2･2　初等的命題

$P(x_1, \cdots, x_n)$ が有理整数を係数とする $x_1, \cdots, x_n$ の多項式であるとき

$$P(x_1, \cdots, x_n)=0$$

で表わされる命題をこの本では初等的な命題とよぶことにする(一般的な用語ではないから注意せよ)。ここでは，初等的な命題についての簡単な性質に 2，3 ふれておこう。

2･2･1　R と S とが初等的な命題であれば

$$R \vee S \quad と \quad R \wedge S$$

も初等的な命題である。

[証明]

$$P_1=0 \vee P_2=0 \leftrightarrow P_1 \cdot P_2=0$$

$$P_1=0 \wedge P_2=0 \leftrightarrow P_1^2+P_2^2=0$$

から明らかであろう。

2·2·2　$R(x, x_1, \cdots, x_n)$ が初等的な命題であれば

$$\forall x \leq y \quad R(x, x_1, \cdots, x_n)$$

は $y, x_1, \cdots, x_n$ についての初等的な命題である。

[証明]　$R(x, x_1, \cdots, x_n)$ は

$$P(x, x_1, \cdots, x_n)=0$$

であるとすれば

$$\forall x \leq y (P(x, x_1, \cdots, x_n)=0 \leftrightarrow \left(\sum_{x=0}^{y} P(x, x_1, \cdots, x_n)^2\right)=0$$

いま

$$P(x, x_1, \cdots, x_n)^2=\sum_{k=0}^{r} P_k(x_1, \cdots, x_n) x^k$$

として

$$\begin{aligned}\forall x \leq y (P(x, x_1, \cdots, x_n)=0) &\leftrightarrow \sum_{x=0}^{y} \sum_{k=0}^{r} P_k(x_1, \cdots, x_n) x^k=0 \\ &\leftrightarrow \sum_{k=0}^{r}\left(P_k(x_1, \cdots, x_n) \sum_{x=0}^{y} x^k\right)=0\end{aligned}$$

ところで

$$\sum_{x=0}^{y} x^k=A_{0,k}+A_{1,k} y+\cdots+A_{k+1,k} y^{k+1}$$

なる形で表わされる。ここに，$A_{i,k}$ は有理数である。いま，十分大きな有理整数 D をとれば，$DA_{0,k}, \cdots, DA_{k+1,k}$ はすべて有理整数となる。ゆえに

$$\forall x \leq y (P(x, x_1, \cdots, x_n)=0 \leftrightarrow \sum_{k=0}^{r} \sum_{j=0}^{k+1} DA_{j,k} P_k(x_1, \cdots, x_n) y^j=0$$

となって証明は終った。

2·2·3　$R(x, x_1, \cdots, x_n)$ が初等的であれば

$$\forall x R(x, x_1, \cdots, x_n)$$

も初等的である。

[証明]　いま

$$R(x,\ x_1,\ \cdots,\ x_n) \leftrightarrow \sum_{k=0}^{r} P_k(x_1,\ \cdots,\ x_n)x^k=0$$

とすれば

$$\forall x R(x,\ x_1,\ \cdots,\ x_n) \leftrightarrow \forall x\Bigl(\sum_{k=0}^{r} P_k(x_1,\ \cdots,\ x_n)x^k=0\Bigr)$$

が得られる。

ところで，この ↔ の左辺において x を仮定すれば，そこで j を非常に大きくとって考えれば最高次の係数 $P_r(x_1,\ \cdots,\ x_n)=0$ であることがわかる。同様にして，順々に

$$P_{r-1}(x_1,\ \cdots,\ x_n),\ P_{r-2}(x_1,\ \cdots,\ x_n),\ \cdots$$

がすべて 0 となることがわかるから

$$\begin{aligned}\forall x R(x,\ x_1,\ \cdots,\ x_n) &\leftrightarrow P_0(x_1,\ \cdots,\ x_n)=0 \land \cdots \land P_r(x_1,\ \cdots,\ x_n)=0\\ &\leftrightarrow \sum_{k=0}^{r}(P_k(x_1,\ \cdots,\ x_n))^2=0\end{aligned}$$

となる。

2·3　diophantine の基本的性質

2·3·1　R と S とが diophantine であれば，$R\land S$ と $R\lor S$ も diophantine である。

[証明]

$$\begin{aligned}&(\exists x_1,\ \cdots,\ x_n Q_1)\lor(\exists y_1,\ \cdots,\ y_m Q_2)\\ &\quad\leftrightarrow \exists x_1,\ \cdots,\ x_n,\ y_1,\ \cdots,\ y_m\ (Q_1\lor Q_2)\\ &(\exists x_1,\ \cdots,\ x_n Q_1)\land(\exists y_1,\ \cdots,\ y_m Q_2)\\ &\quad\leftrightarrow \exists x_1,\ \cdots,\ x_n,\ y_1,\ \cdots,\ y_m\ (Q_1\land Q_2)\end{aligned}$$

と 2·2·1 より明らか。

2·3·2　R が diophantine であるならば $\exists x_1,\ \cdots,\ x_n R$ も diophantine である。

[証明]　明らか。

2·3·3　$x\neq 0$ は diophantine である。

[証明] $$x \neq 0 \leftrightarrow \exists y(x-y-1=0)$$

2・3・4 $x<y$ は diophantine である。

[証明] $$x<y \leftrightarrow \exists z(z \neq 0 \wedge y-x-z=0)$$

2・3・5 $x \neq y$ は diophantine である。

[証明] $$x \neq y \leftrightarrow x<y \vee y<x$$

2・3・6 $x \equiv y \pmod z$ は diophantine である。

[証明] $$x \equiv y \pmod z \leftrightarrow \exists w(x-y-zw=0 \vee x-y+zw=0)$$

2・3・7 $z=J(x, y)$ は diophantine である。

[証明] $$z=J(x, y) \leftrightarrow 2z-x^2-y^2-2xy-3x-y=0$$

2・4　方程式 $x^2-(a^2-1)y^2=1$ の解

さて，diophantine についていくぶん深い性質を導くために，Pell の方程式

$$x^2-(a^2-1)y^2=1$$

を考えることにする。

ほとんど明らかなことであろうが，自然数を考えるかわりに正の自然数のみを考えてもわれわれの問題にはほとんどかわりはない。たとえば，帰納的可算とか，第 10 問題とかは正の自然数だけにかぎっても実質的にはなんのかわりもないことは明らかであろう。したがって，以下本章では，変数は断わらないかぎりすべて正の自然数を表わすものとする。さて，まず

$$x^2-(a^2-1)y^2=1$$

のすべての根を求めることを考えよう。ここに，x, y は正の自然数である。$a=1$ のときは，問題は自明になってしまうので，$a>1$ と仮定しよう。

さて

$$(a+\sqrt{a^2-1})(a-\sqrt{a^2-1})=1$$

であるから

$$(a+\sqrt{a^2-1})^n(a-\sqrt{a^2-1})^n=1$$

となる。

いま，$(a+\sqrt{a^2-1})^n$ を展開して

$$x_n(a)+y_n(a)\sqrt{a^2-1}$$

とすれば($x_n(a)$, $y_n(a)$ は a の多項式)，$(a-\sqrt{a^2-1})^n$ の展開は

$$x_n(a)-y_n(a)\sqrt{a^2-1}$$

となるから

$$(x_n(a))^2-(a^2-1)(y_n(a))^2=1$$

となり，$x_n(a)$, $y_n(a)$ が $x^2-(a^2-1)y^2=1$ の解であることがわかる。ここに，$x_n(a)$, $y_n(a)$ が正であることは明らかであろう。

つぎに，この逆を証明しよう。

定理 1　$x^2-(a^2-1)y^2=1$ の解は $x_n(a)$, $y_n(a)$ の形で表わされる。

[証明]　u, v を有理整数を表わす変数として，$v\neq 0$ で

$$u^2-(a^2-1)v^2=1$$

が満たされているものとする。すなわち

$$(u+v\sqrt{a^2-1})(u-v\sqrt{a^2-1})=1$$

が得られる。

u, v は正でも負でもよいが，$u+v\sqrt{a^2-1}$, $u-v\sqrt{a^2-1}$ は正で，しかも

$$u-v\sqrt{a^2-1}<1<u+v\sqrt{a^2-1}$$

が成立しているものとする(そうでなければ，v の符号を逆にすればよい)。このとき

$$a+\sqrt{a^2-1}\leqq u+v\sqrt{a^2-1}$$

が成立することを証明する。そのために，逆を仮定して矛盾を導こう。

$$1<u+v\sqrt{a^2-1}<a+\sqrt{a^2-1}$$

$$a-\sqrt{a^2-1}<u-v\sqrt{a^2-1}<1$$

となる。これを変形すると

$$0<2v\sqrt{a^2-1}<2\sqrt{a^2-1}$$

となり，ゆえに $0<v<1$ となって矛盾する。

さて，つぎに $u=x_n(a)$, $v=y_n(a)$ なる n が存在することを証明しよう。明らかに

$$x_n(a)+y_n(a)\sqrt{a^2-1}\leq u+v\sqrt{a^2-1}<x_{n+1}(a)+y_{n+1}(a)\sqrt{a^2-1}$$

なる n が存在する。これから

$$1\leq(u+v\sqrt{a^2-1})(x_n(a)-y_n(a)\sqrt{a^2-1})<a+\sqrt{a^2-1}$$

が得られる。

ところで

$$\begin{aligned}&(u+v\sqrt{a^2-1})(x_n(a)-y_n(a)\sqrt{a^2-1})\\&=(ux_n(a)-vy_n(a)(a^2-1))+(vx_n(a)-uy_n(a))\sqrt{a^2-1}\end{aligned}$$

であり，また

$$\begin{aligned}&(ux_n(a)-vy_n(a)(a^2-1))^2-(vx_n(a)-uy_n(a))^2(a^2-1)\\&=(u^2-(a^2-1)v^2)x_n{}^2(a)-(u^2-(a^2-1)v^2)y_n{}^2(a)(a^2-1)\\&=1\end{aligned}$$

となるから，上に証明したことにより

$$1=(u+v\sqrt{a^2-1})(x_n(a)-y_n(a)\sqrt{a^2-1})$$

となり

$$u+v\sqrt{a^2-1}=x_n(a)+y_n(a)\sqrt{a^2-1}$$

が証明された。

つぎに，$x_n(a)$, $y_n(a)$ についての簡単な性質を述べよう。上の定理の証明の中では一般の有理整数 u, v を用いたが，今後はまた変数は常に正の自然数を表わすものとする。明らかなものは証明をはぶく。

2・4・1 $$x_0(a)=1,\quad x_1(a)=a,\quad x_2(a)=2a^2-1$$
$$y_0(a)=0,\quad y_1(a)=1,\quad y_2(a)=2a$$

2・4・2 $$x_0(a)<x_1(a)<x_2(a)<\cdots$$
$$y_0(a)<y_1(a)<y_2(a)<\cdots$$

ここで，$1<a$ を用いている。

2・4・3 $$x_{n+1}(a)=a\cdot x_n(a)+(a^2-1)y_n(a)$$
$$y_{n+1}(a)=x_n(a)+a\cdot y_n(a)$$

［証明］ $$\begin{aligned}&(x_n(a)+y_n(a)\sqrt{a^2-1})(a+\sqrt{a^2-1})\\&=(a\cdot x_n(a)+(a^2-1)y_n(a))+(x_n(a)+a\cdot y_n(a))\sqrt{a^2-1}\end{aligned}$$

2·4·4 $$x_{n+1}(a)=2a\cdot x_n(a)-x_{n-1}(a)$$
$$y_{n+1}(a)=2a\cdot y_n(a)-y_{n-1}(a)$$

[証明] $n=1$ のときは 2·4·1 より明らか。あとは n についての帰納法を用いる。n のときを仮定して，$n+1$ のときは

$$\begin{aligned}
x_{n+2}(a)&=a\cdot x_{n+1}(a)+(a^2-1)y_{n+1}(a) && (2\cdot4\cdot3)\\
&=a\cdot x_{n+1}(a)+(a^2-1)(x_n(a)+a\cdot y_n(a)) && (2\cdot4\cdot3)\\
&=a\cdot x_{n+1}(a)-x_n(a)+a(a\cdot x_n(a)+(a^2-1)y_n(a))\\
&=a\cdot x_{n+1}(a)-x_n(a)+a\cdot x_{n+1}(a) && (2\cdot4\cdot3)\\
y_{n+2}(a)&=x_{n+1}(a)+a\cdot y_{n+1}(a) && (2\cdot4\cdot3)\\
&=a(x_n(a)+a\cdot y_n(a))-y_n(a)+a\cdot y_{n+1}(a) && (2\cdot4\cdot3)\\
&=a(x_n(a)+a\cdot y_n(a))-y_n(a)+a\cdot y_{n+1}(a) && (2\cdot4\cdot3)\\
&=a\cdot y_{n+1}(a)-y_n(a)+a\cdot y_{n+1}(a) && (2\cdot4\cdot3)
\end{aligned}$$

2·4·5 $x_0(a),\ x_2(a),\ x_4(a),\ \cdots,\ x_{2n}(a),\ \cdots$ は奇数である

$y_1(a),\ y_3(a),\ y_5(a),\ \cdots,\ y_{2n+1}(a),\ \cdots$ は奇数である

$y_0(a),\ y_2(a),\ y_4(a),\ \cdots,\ y_{2n}(a),\ \cdots$ は偶数である

[証明] 2·4·1 と 2·4·4 より明らか。

2·4·6 $$y_{m+n}(a)=x_n(a)y_m(a)+x_m(a)y_n(a)$$

[証明] $$x_{m+n}(a)+y_{m+n}(a)\sqrt{a^2-1}$$
$$=(x_n(a)+y_n(a)\sqrt{a^2-1})(x_m(a)+y_m(a)\sqrt{a^2-1})$$

以下，a を固定して，$x_n(a)$，$y_n(a)$ を単に x_n，y_n とかくことにしよう。

2·4·7 $$(x_n,\ y_n)=1$$

[証明] ${x_n}^2-(a^2-1){y_n}^2=1$ より明らか。

2·4·8 $$y_n \mid y_t \leftrightarrow n \mid t$$

[証明] 2·4·6 により

$$y_{nk+n}=x_n y_{nk}+x_{nk} y_n$$

であるから，数学的帰納法により $y_n \mid y_{nk}$ は明らかである。

つぎに，$y_n \mid y_t$，$n \nmid t$ として矛盾を出そう。

$$t=nq+r \qquad (0<r<n)$$

とすれば，2·4·6 より

$$y_t = x_r y_{nq} + x_{nq} y_r$$

となる。

ところで，$y_n \mid y_{nq}$ であるから，2·4·7 により $y_n \mid y_r$ となるが，$r<n$ であるからこれは 2·4·2 に反する。

2·4·9　$$y_{nk} \equiv k x_n^{k-1} y_n \qquad (\mathrm{mod}\,(y_n)^3)$$

［証明］　$x_{nk}+y_{nk}\sqrt{a^2-1}=(x_n+y_n\sqrt{a^2-1})^k$ を計算すれば

$$y_{nk}=\sum_{\substack{j=1\\ j\text{は奇数}}}^{k}\binom{k}{j}x_n^{k-j}y_n^j(a^2-1)^{(j-1)/2}$$

これから明らかであろう。

2·4·10　$$y_k \equiv k \qquad (\mathrm{mod}\, a-1)$$

［証明］　2·4·9 の証明の展開式を $n=1$ としてながめれば明らか。$x_1=a$, $y_1=1$, $a\equiv 1$ $(\mathrm{mod}\, a-1)$ に注意せよ。

2·4·11　$$y_n^2 \mid y_{n \cdot y_n}$$

またさらに

$$y_n^2 \mid y_t$$

ならば

$$y_n \mid t$$

である。

［証明］　最初の式は，2·4·9 に $k=y_n$ とおけば得られる。

つぎに $y_n^2 \mid y_t$ を仮定すれば，2·4·8 により $n \mid t$ となる。したがって，$t=nk$ とおけば 2·4·9 によってつぎの式が得られる。

$$y_n \mid k x_n^{k-1}$$

ところで，2·4·7 により $y_n \mid k$, したがって $y_n \mid t$ となる。

2·4·12　$$y_{k+u} \equiv -y_{k+1-u} \qquad (\mathrm{mod}\, y_k+y_{k+1})$$

［証明］　$u=0, 1$ のときは明らかである。一般には，u についての数学的帰納法によって証明する。すなわち，u のときを仮定して，$u+1$ のときは

$$\begin{aligned} y_{k+u+1} &= 2a y_{k+u} - y_{k+u-1} && (2\cdot4\cdot4)\\ &\equiv -2a y_{k+1-u} + y_{k+1-(u-1)} && (\mathrm{mod}\, y_k+y_{k-1}) \end{aligned}$$

$$=-y_{k+1-(u+1)} \qquad (2\cdot4\cdot4)$$

ここで，第2行目は帰納法の仮定を用いたのである。

2・4・13

$$y_{2k+1}\equiv 0 \pmod{y_k+y_{k+1}}$$
$$y_{2k}\equiv -1 \pmod{y_k+y_{k+1}}$$
$$y_{2k+2}\equiv 1 \pmod{y_k+y_{k+1}}$$

[証明]　最初の2式は，2・4・12 において $u=k+1, k$ とおけばよい。最後の式は，この2式と 2・4・4 により得られる。

$$y_{2k+2}=2ay_{2k+1}-y_{2k}\equiv -1 \pmod{y_k+y_{k+1}}$$

2・4・14　y_i $(0\leq i<2k+1)$ のどの相異なるものをとっても，$\bmod y_k+y_{k+1}$ で同等ではない。

[証明]　$k+1\leq i<2k+1$ ならば，2・4・12 により $y_i\equiv -y_j$ $(j\leq k)$ となるから，y_0，y_1，$\cdots$，y_{2k} は全体として

$$-y_k<\cdots<-y_2<-y_1<y_0<y_1<\cdots<y_k$$

のいずれか1つと $\bmod y_k+y_{k+1}$ で同等であるが，しかしこのいずれも互いに同等でないことは明らかである。

2・4・15

$$y_{n+2k+1}\equiv y_n \pmod{y_k+y_{k+1}}$$

[証明]　$n=0, 1$ のときは，2・4・13 から得られる。一般のときは，n についての数学的帰納法によって証明する。n のとき成立しているとして，$n+1$ のときを，2・4・4 を用いて証明する。

$$\begin{aligned} y_{(n+1)+2k+1} &= 2ay_{n+2k+1}-y_{(n-1)+2k+1} \\ &\equiv 2ay_n-y_{n-1} \pmod{y_k+y_{k+1}} \\ &= y_{n+1} \end{aligned}$$

2・4・16　$y_{2k+1}=(y_{k+1}-y_k)(y_{k+1}+y_k)$

[証明]

$$\begin{aligned} y_{2k+1} &= y_kx_{k+1}+x_ky_{k+1} && (2\cdot4\cdot6) \\ &= y_k(ax_k+(a^2-1)y_k)+x_ky_{k+1} && (2\cdot4\cdot3) \\ &= ay_k(x_k+ay_k)+x_ky_{k+1}-y_k{}^2 && \\ &= ay_ky_{k+1}+x_ky_{k+1}-y_k{}^2 && (2\cdot4\cdot3) \\ &= y_{k+1}{}^2-y_k{}^2 && (2\cdot4\cdot3) \end{aligned}$$

2･4･17　　$(y_{k+1}+y_k,\ y_{k+1}-y_k)=1$

［証明］　もし素数pが$y_{k+1}+y_k$と$y_{k+1}-y_k$とを割るものとすれば，$p\mid 2y_{k+1}$で$p\mid 2y_k$となる。ところで，2･4･5によりy_{2k+1}は奇数であるから，2･4･16によってpも奇の素数である。ゆえに，$p\mid y_{k+1}$，$p\mid y_k$となる。ゆえに，2･4･3の第2式により$p\mid x_k$となる。ところで，2･4･7により$(x_k, y_k)=1$であるから矛盾する。

2･4･18　$2s+1\mid 2n+1$であるとすれば

$$y_{s+1}+y_s\mid y_{n+1}+y_n \quad \text{で} \quad y_{s+1}-y_s\mid y_{n+1}-y_n$$

である。

［証明］　いま，$2n+1=q(2s+1)$とおけば，$q=1$のときは明らかである。qは奇数であるから，qに対して成立すると仮定して，$q+2$に対しても成立することを証明すれば十分である。

$$\begin{aligned}(q+2)(2s+1)&=2n+1+4s+2\\&=2(n+2s+1)+1\end{aligned}$$

$$\begin{aligned}&y_{n+2s+2}\pm y_{n+2s+1}\\&=(y_{n+1}x_{2s+1}+x_{n+1}y_{2s+1})\pm(y_nx_{2s+1}+x_ny_{2s+1})\\&=x_{2s+1}(y_{n+1}\pm y_n)+(y_{s+1}-y_s)(y_{s+1}+y_s)(x_{n+1}\pm x_n) \qquad (2\cdot4\cdot16)\end{aligned}$$

数学的帰納法により，命題は明らかであろう。

2･4･19　$2n+1=(2s+1)y_{2s+1}$とnを定義すれば(2･4･5に注意)

（i）　$(y_{s+1}-y_s)^2\mid y_{n+1}-y_n$

（ii）　$(y_{s+1}+y_s)^2\mid y_{n+1}+y_n$

（iii）　$(y_{s+1}-y_s,\ y_{n+1}+y_n)=(y_{s+1}+y_s,\ y_{n+1}-y_n)=1$

である。

［証明］　2･4･11と2･4･16とにより

$$(y_{s+1}-y_s)^2(y_{s+1}+y_s)^2\mid(y_{n+1}-y_n)(y_{n+1}+y_n)$$

したがって，(iii)が証明されれば，(i)，(ii)は明らかである。

(iii)を証明するために，pは素数でしかも$y_{s+1}-y_s$と$y_{n+1}+y_n$の公約数であるとすれば，pは2･4･18により$y_{n+1}-y_n$と$y_{n+1}+y_n$の公約数となり2･4･7

に矛盾する。$(y_{s+1}+y_s,\ y_{n+1}-y_n)=1$ も同様にして証明される。

2·5　$v=y_u(a)$ は diophantine である

本節のおもな目的は，つぎの定理の証明である。

定理 1　$v=y_u(a)$ は diophantine である。

定理の証明のために，まず補題を2つ証明する。

補題 1

$$a\equiv b \pmod c$$

ならば

$$y_n(a)\equiv y_n(b) \pmod c$$

である。

[証明]　$y_n(a)$ は整係数の a の多項式であるから明らか。

補題 2　いま

$$v\leq y_k(a)$$
$$y_k(a)+y_{k+1}(a)\mid m-a$$
$$y_n(m)\equiv v \pmod{y_k(a)+y_{k+1}(a)}$$

の3条件が満たされているとすれば，ある j でつぎの条件を満たすものが存在する。

$$v=y_j(a)$$

で

$$n\equiv j \pmod{2k+1}$$

である。

[証明]　補題1により

$$y_n(m)\equiv y_n(a) \pmod{m-a}$$

仮定により

$$y_n(m)\equiv y_n(a) \pmod{y_k(a)+y_{k+1}(a)}$$

ゆえに，仮定により

$$v\equiv y_n(a) \pmod{y_k(a)+y_{k+1}(a)}$$

となる。

ところで，2·4·14 と 2·4·15 とにより

$$v \equiv y_j(a) \qquad (\mathrm{mod}\; y_k(a)+y_{k+1}(a))$$

で，$j \leq k$ である j がただ1つ存在する。この j をとれば

$$v \equiv y_j(a) \qquad (\mathrm{mod}\; y_k(a)+y_{k+1}(a))$$

で，$v \leq y_k(a)$ であるから $v=y_j(a)$ となり

$$y_n(a) \equiv y_j(a) \qquad (\mathrm{mod}\; y_k(a)+y_{k+1}(a))$$

と 2·4·14 および 2·4·15 とにより

$$n \equiv j \qquad (\mathrm{mod}\; 2k+1)$$

が出てくる。

さて，いよいよ定理1の証明をすることにしよう。まず，つぎの連立方程式を考えよう。

I $u+j-1=v$

II a $p+(a-1)q=v+r$

II b $g=v+t$

III $p^2-(a^2-1)q^2=1$

IV a $h+(a+1)g=b(p+(a+1)q)^2$

IV b $h+(a-1)g=c(p+(a-1)q)^2$

V $h^2-(a^2-1)q^2=1$

VI $m=(h+(a+1)g)z+a$

VII $m=f(p+(a-1)q)+1$

VIII $x^2-(m^2-1)y^2=1$

IX $y=(d-1)(p+(a-1)q)+u$

X $y=(e-1)(h+(a+1)g)+v$

$v=y_u(a)$ が，I～X までの連立方程式において a, u, v 以外の変数についての根が存在するという命題と同等であることを証明しよう。この連立方程式に根が存在するという命題は diophantine であることは明らかであるから，これから定理1はただちに出てくる。

まず，I～X が満たされているとして，$v=y_u(a)$ が成立することを証明しよ

う。まず，定理1と III, V からつぎの条件を満たす s と k が存在することがわかる。

$$p=x_s(a), \qquad q=y_s(a)$$
$$h=x_k(a), \qquad g=y_k(a)$$

いま，l, l', N, N' を

$$l=p+(a-1)q, \qquad N=h+(a-1)g$$
$$l'=p+(a+1)q, \qquad N'=h+(a+1)g$$

によって定義すれば，2・4・3 によって

$$l=y_{s+1}(a)-y_s(a), \qquad N=y_{k+1}(a)-y_k(a)$$
$$l'=y_{s+1}(a)+y_s(a), \qquad N'=y_{k+1}(a)+y_k(a)$$

が得られる。さらに変数が正であることと I, II a, b から，つぎの式が得られる。

$$u\leq v<l, \qquad v<g \tag{1}$$

IV a, b と l, l', N, N' の定義から，つぎの式が得られる。

$$l^2 \mid N, \qquad l'^2 \mid N'$$

この式と 2・4・16 とから

$$y_{2s+1}{}^2 \mid y_{2k+1}$$

となり，これに 2・4・11 の後半を用いて

$$y_{2s+1} \mid 2k+1$$

したがって

$$l \mid 2k+1 \tag{2}$$

となる。VI, VII から，つぎの合同式が得られる。

$$m\equiv\begin{cases} a & (\bmod N') \\ 1 & (\bmod l) \end{cases} \tag{3}$$

VIII から，$y=y_n(m)$ となる n が存在することがわかる。

最後に，IX, X からつぎの合同式が得られる。

$$y\equiv\begin{cases} u & (\bmod l) \\ v & (\bmod N') \end{cases} \tag{4}$$

(1)〜(4)によって，補題2の仮定がすべて満たされていることがわかるから

$$v=y_{j'}(a),\quad n\equiv j' \qquad (\mathrm{mod}\ 2k+1)$$

なる j' が存在する。

(2)により

$$n\equiv j' \qquad (\mathrm{mod}\ l) \tag{5}$$

2·4·10 および(3)と $y=y_n(n)$ とにより

$$y\equiv n \qquad (\mathrm{mod}\ l) \tag{6}$$

(4), (5), (6)により

$$u\equiv j' \qquad (\mathrm{mod}\ l)$$

となる。

ところで，(1)により

$$u<l \quad で \quad j'\leq y_{j'}(a)=v<l$$

であるから，$u=j'$ となり $v=y_n(a)$ が出てきて，証明された。

今度は逆に，$v=y_n(a)$ を仮定して I〜X を満たす解が存在することを証明することにしよう。

まず第1に，$u\leq v$ であるから I を満たす j をとることができる。つぎに，$y_s(a)>v$ となる s をとって $p=x_s(a)$, $q=y_s(a)$ とおけば，III は満たされ，また IIa を満たす r をとることができる。

k を $2k+1=(2s+1)y_{2s+1}(a)$ と定義して，$h=x_k(a)$, $g=x_k(a)$ とおけば，$g\geq q>v$ であるから IIb は満たされており，さらに V も満たされている上に，2·4·19 により IVa, b を満たす b, c が存在することがわかる。さらに前と同様に，l, l', N, N' を定義すれば，やはり 2·4·19 によって $(N', l)=1$ も出てくる。

したがって，剰余定理によりつぎの条件を満たす m が存在する。

$$m\equiv a \qquad (\mathrm{mod}\ N')$$

$$m\equiv 1 \qquad (\mathrm{mod}\ l)$$

$$m>a$$

ゆえに，VI, VII を満たすように z と f をとることができる。

$$x=x_u(m), \qquad y=y_u(m)$$

とおけば，VIII は満たされる。

補題 1 と VI とにより

$$y\equiv v \qquad (\mathrm{mod}\, N')$$

であるから，X を満たすように e をとることができる($m>a$ に注意)。

最後に，$y_u(1)=u$ と補題 1 および VII とにより

$$y\equiv u \qquad (\mathrm{mod}\, l)$$

となるから，IX を満たすように ($u\leq v$ に注意) d をとることができて，証明が終った。

2·6 $\alpha=\beta^u$ は diophantine である

本節の目的は，つぎの定理の証明である。

定理 1 $\alpha=\beta^u$ は diophantine である。

この定理を証明するために，まず 2 つの補題の証明をすることにする。

補題 1 $x_n(a)-y_n(a)(a-y)\equiv y^n \qquad (\mathrm{mod}\, 2ay-y^2-1)$

[証明] $x_n(a)-y_n(a)(a-y)-y^n$ を y の多項式として $2ay-y^2-1$ で割って(y^2 の係数が -1 であるから割り算は a の多項式の係数でできる)

$$x_n(a)-y_n(a)(a-y)-y^n=P(a, y)(2ay-y^2-1)+f(a)y+g(a)$$

とする。この y に $a+\sqrt{a^2-1}$ を代入すれば，左辺と右辺の第 1 項は 0 となるから

$$f(a)a+f(a)\sqrt{a^2-1}+g(a)=0$$

この等式は a を変数として成立するから，$f(a)=0$, $g(a)=0$ が出て，証明は終った。

補題 2 (i) $x_n(a)\geq a^n$

(ii) $y>1$ で $a>y^n$ ならば，$2ay-y^2-1>y^n$。

[証明] (i) は $x_{n+1}(a)\geq a\cdot x_n(a)$ より明らかである(2·4·4 参照)。

(ii) は $y>1$, $a>y^n$ ならば $2ay>2y^{n+1}+1>y^n+y^2+1$。

さて定理の証明をするために，前節の I～X につぎの XI～XV をつけ加え

た連立方程式を考えよう。

XI $w^2-(a^2-1)v^2=1$

XII $w-v(a-\beta)=\alpha+(\gamma-1)(2a\beta-\beta^2-1)$

XIII $\alpha+\delta=2a\beta-\beta^2-1$

XIV a $\beta+\zeta=\eta$

XIV b $u+\xi=\eta$

XV $a^2-(\eta^2-1)(\eta-1)^2\delta^2=1$

$\alpha=\beta^u$ と，I～XV の連立方程式の α, β, u 以外の変数に根があることとが同等であることを証明しよう。I～XV の連立方程式に根があるという命題が diophantine であることは明らかであるから，このことから定理はただちに出てくる。

まず，I～XV に根があるとして $\alpha=\beta^u$ を導こう。まず前節の定理により，$v=y_u(a)$ となり，さらに XI により $w=x_u(a)$ となる。

補題1と XII により，つぎの式が成立する。

$$\alpha\equiv\beta^u \pmod{2a\beta-\beta^2-1} \qquad (1)$$

XIII により

$$\alpha<2a\beta-\beta^2-1 \qquad (2)$$

XIV a, b により

$$\beta,\ u<\eta$$

XV により，つぎの式を満たす n が存在する。

$$a=x_n(\eta), \qquad (\eta-1)\delta=y_n(\eta)$$

これと 2·4·10 により

$$n\equiv 0 \pmod{\eta-1}$$

ゆえに

$$\eta-1\leq n$$

となる。ゆえに，補題2の（i）により

$$a\geq\eta^{\eta-1}>\beta^u$$

これから，もし $\beta>1$ ならば補題2の（ii）により $\beta^u<2a\beta-\beta^2-1$ であるか

ら，(1), (2) により $\alpha=\beta^u$ となって証明が終った。

ゆえに $\beta=1$ とすれば，(1) により

$$\alpha\equiv 1 \pmod{2a-2}$$

となる。

ところで，(2) により $\alpha<2a-2$ となるから，$\alpha=1$ となって証明された。

つぎに，$\alpha=\beta^u$ として I〜XV を満たす根があることを証明しよう。

まず，$\eta>\beta$, $\eta>a$ なる η をとって $a=x_{\eta-1}(\eta)$ とおけば，2·4·10 により

$$y_{\eta-1}(\eta)\equiv 0 \pmod{\eta-1}$$

であるから，XV を満たすような δ が存在することがわかる。さらに，XIV a, XIV b を満たすような ζ, ξ が存在することは明らかである。

XIII を満たすような δ が存在することは，$\beta>1$ ならば補題 2 の (ii) からただちにわかる。また，$\beta=1$ ならば $\alpha=1$ であるから明らかである。

したがって，$w=x_u(a)$, $v=y_u(a)$ とおけば XI は満たされ，さらに XII を満たすような δ が存在することが補題 1 よりわかる。さらに，この a, u, v について前節の I〜X を満たすような根をとればよいから，定理は証明された。

2·7 $y=x!$ は diophantine である

ここでは，表題に関係した 3 つの性質を証明する。

2·7·1 $r=\binom{n}{k}$ は diophantine である。

[証明] いま，$0<k\leq n$ とすれば

$$\begin{aligned}2^{nk}(1+2^{-n})^n &= 2^{nk}\sum_{\nu=0}^{n}\binom{n}{\nu}2^{-n\nu}\\ &= \sum_{\nu=0}^{k}\binom{n}{\nu}2^{n(k-\nu)}+2^{-n}\sum_{\nu=k+1}^{n}\binom{n}{\nu}2^{-n(\nu-k-1)}\\ &< \sum_{\nu=0}^{k}\binom{n}{\nu}2^{n(k-\nu)}+2^{-n}\left(\sum_{\nu=0}^{n}\binom{n}{\nu}-1\right)\\ &= \sum_{\nu=0}^{k}\binom{n}{\nu}2^{n(k-\nu)}+\frac{2^n-1}{2^n}\end{aligned}$$

したがって，$[a]$ を，a をこえない最大の有理整数とすれば

$$\left[2^{nk}(1+2^{-n})^n\right]=\sum_{\nu=0}^{k}\binom{n}{\nu}2^{n(k-\nu)}$$

となる。

同様にして

$$2^n\left[2^{n(k-1)}(1+2^{-n})^n\right]=\sum_{\nu=0}^{k-1}\binom{n}{\nu}2^{n(k-\nu)}$$

ゆえに

$$\binom{n}{k}=\left[2^{nk}(1+2^{-n})^n\right]-2^n\left[2^{n(k-1)}(1+2^{-n})^n\right]$$

が得られる。したがって，$r=\binom{n}{k}$ はつぎの式と同等である。

$$\begin{aligned}(n\leq k\wedge r=1)\vee(k<n\wedge \exists u, v(r=u-2^n v\\ \wedge 2^{n^2}u\leq 2^{nk}(1+2^n)^n<2^{n^2}(1+u)\\ \wedge 2^{n^2}v\leq 2^{n(k-1)}(1+2^n)^n<2^{n^2}(1+v)))\end{aligned}$$

ところで，この式が diophantine であることは明らかである。

2·7·2 $y=x!$ は diophantine である。

[証明] まず，$0<\theta<\dfrac{1}{2}$ とすれば

$$(1-\theta)(1+2\theta)=1+\theta-2\theta^2>1$$

したがって

$$\frac{1}{1-\theta}<1+2\theta \qquad \left(0<\theta<\frac{1}{2}\right)$$

つぎに，$0<\theta<1$ とすれば，正の自然数 x に対して

$$\frac{(1+\theta)^x-1}{\theta}=\sum_{k=1}^{x}\binom{x}{k}\theta^{k-1}<\sum_{k=0}^{x}\binom{x}{k}=2^x$$

したがって

$$(1+\theta)^x<1+2^x\theta \qquad (0<\theta<1)$$

が得られる。

いま，r を $(2x)^{x+1}$ より大きい任意の自然数とすれば

$$\begin{aligned}\frac{r^x}{\binom{r}{x}}&=\frac{x!}{\left(1-\frac{1}{r}\right)\left(1-\frac{2}{r}\right)\cdots\left(1-\frac{x-1}{r}\right)}\\ &<\frac{x!}{\left(1-\frac{x}{r}\right)^x}<x!\left(1+\frac{2x}{r}\right)^x\end{aligned}$$

$$<x!\left(1+2^x\cdot\frac{2x}{r}\right)<x!+1$$

ところで，明らかに

$$x!<\frac{x!}{\left(1-\dfrac{1}{r}\right)\left(1-\dfrac{2}{r}\right)\cdots\left(1-\dfrac{x-1}{r}\right)}$$

ゆえに

$$x!=\left[\frac{r^x}{\binom{r}{x}}\right]$$

が得られる。したがって，$y=x!$ はつぎの式と同等である。

$$y\binom{(2x)^{x+1}+1}{x}<\left((2x)^{x+1}+1\right)^x<y\binom{(2x)^{x+1}+1}{x}+1$$

この式が diophantine であることは明らかであろう。

2・7・3 ‘p は素数である’ は diophantine である。

[証明] ‘p は素数である’ は，$p>1$ で p が $(p-1)!$ と互いに素であるということと同等であるから，つぎの式と同等である。

$$\exists u,v(p>1\wedge(pu-(p-1)!\,v=1\vee -pu+(p-1)!\,v=1))$$

この式が diophantine であることは明らかであろう。

2・8 重要な補助定理

この節の終りに重要な補助定理を証明する。その準備として，まず2,3の補題を証明する。最初に，α が有理数のときまで拡張して，$\binom{\alpha}{k}$ を

$$\binom{\alpha}{k}=\frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$$

と定義する。

補題 1 命題

$$\frac{x}{y}=\binom{p/q}{k}\wedge p>qk$$

は diophantine である。

[証明] いま，$\alpha=p/q$ で $\alpha>k$ とすれば，Taylor 展開により

$$a^{2k+1}(1+a^{-2})^{\alpha}=\sum_{j=0}^{k}\binom{\alpha}{j}a^{2k-2j+1}+\binom{\alpha}{k+1}a^{-1}(1+\theta a^{-2})^{\alpha-k+1}$$

で，$0<\theta<1$ となる。ところで

$$\frac{\binom{\alpha}{k+1}}{\alpha^{k+1}}<1$$

$$\frac{(1+\theta a^{-2})^{\alpha-k-1}}{2^{\alpha-1}}<\frac{1}{(1+\theta a^{-2})^{k}}<1$$

となるから，$0<\theta'<1$ なる θ' でつぎの式を満たすものがある。

$$a^{2k+1}(1+a^{-2})^{\alpha}=\sum_{j=0}^{k}\binom{\alpha}{j}a^{2k-2j+1}+\theta'\alpha^{k+1}a^{-1}2^{\alpha-1}$$

いま，$S_k(a)$ をつぎの式によって定義する。

$$S_k(a)=\sum_{j=0}^{k}\binom{\alpha}{j}a^{2k-2j+1}$$

a を上手にとってきて

$$S_k(a)=[a^{2k+1}(1+a^{-2})^{p/q}]$$

$$S_{k-1}(a)=[a^{2k-1}(1+a^{-2})^{p/q}]$$

となるようにすれば

$$\binom{p/q}{k}=a^{-1}S_k(a)-aS_{k-1}(a) \qquad (1)$$

と表わすことができる。

いま，$q^k k!\mid a$ であるとすれば，$\binom{p/q}{j}$ の分母はすべて $q^k k!$ の約数であり，$S_k(a)$ および $S_{k-1}(a)$ のすべての項に a が少なくとも1乗ははいってくるので，$S_k(a)$, $S_{k-1}(a)$ はともに有理整数になる。さらに，$a>2^{p-1}p^{k+1}$ をとれば，$\theta'\alpha^{k+1}a^{-1}2^{\alpha-1}<1$ となるから，$a=2^p p^{k+1}q^k k!$ とおけばよい。すなわち，a をこのようにおいた上で

$$u=S_k(a) \leftrightarrow u\le a^{2k+1}(1+a^{-2})^{p/q}<u+1$$

$$\leftrightarrow a^{2p}u^q\le a^{(2k+1)q}(a^2+1)^p<a^{2p}(u+1)^q$$

となって，$u=S_k(a)$ が diophantine であることがわかる。ゆえに，(1)によりつぎの補題が容易に得られる。

補題 2　$y=\prod_{k\le K}(a+bk)$ は diophantine である。

[証明] つぎの式から明かであろう。

$$\prod_{k\leq K}(a+bk)=\binom{a/b+K}{K}b^kK!$$

補題 3 $F(x, y, k, z_1, \cdots, z_m)$ は有理整数を係数とする $x, y, k, z_1, \cdots, z_m$ の多項式とする。そのとき，つぎの命題

$$\forall k\leq y\exists z_1\leq y \cdots \exists z_m\leq y(F(x, y, k, z_1, \cdots, z_m)=0)$$

は diophantine である。

[証明] いま，F の係数の絶対値の和を c とし，F の最高次の次数を $n>0$ とするとき，$G(x, y)=cx^ny^n$ とおけば $G(x, y)\geq y$ で，さらに

$$\forall k\leq y\forall z_1\leq y \cdots \forall z_m\leq y|F(x, y, k, z_1, \cdots, z_m)|\leq G(x, y)$$

が成立する。補題を証明するために，まずつぎの同等を証明する。

$$\begin{aligned}&\forall k\leq y\exists z_1\leq y \cdots \exists z_m\leq y(F(x, y, k, z_1, \cdots, z_m)=0)\\ \leftrightarrow &\exists c, t, a_1, \cdots, a_m(t=G(x, y)!\wedge(1+ct)=\prod_{k\leq y}(1+kt)\\ &\wedge(1+ct)|F(x, y, c, a_1, \cdots, a_m)\wedge(1+ct)|\prod_{j\leq y}(a_1-j)\\ &\wedge(1+ct)|\prod_{j\leq y}(a_2-j)\wedge\cdots\wedge(1+ct)|\prod_{j\leq y}(a_m-j))\end{aligned}$$

まず最初に，右辺が左辺を導くことをいうために，右辺を仮定しよう。

いま，$k\leq y$ で $1+kt$ を割る任意の素数を p_k として，z_{ki} をつぎのように定義しよう。

$$\mathrm{Rem}(a_i, p_k)=z_{ki} \qquad (i=1, \cdots, m)$$

このとき，つぎの 2 式を証明すれば十分である。

$$F(x, y, k, z_{k1}, \cdots, z_{km})=0$$

$$0<z_{ki}\leq y \qquad (i=1, \cdots, m)$$

$p_k|(1+ct)$ であるから

$$p_k|\prod_{j=y}(a_i-j)$$

したがって，ある $1\leq j\leq y$ なる j に対して

$$p_k | a_i-j$$

となる。したがって

$$0 \leq z_{ki} = \mathrm{Rem}(a_i,\ p_k) \leq y$$

で後半がいえた。さて，さらに $(p_k,\ t)=1$ で $t=G(x,\ y)!$ であるから

$$y \leq G(x,\ y) < p_k$$

したがって，$1 \leq z_{ki} \leq y$ であるから

$$|F(x,\ y,\ k,\ z_{k1},\ \cdots,\ z_{km})| \leq G(x,\ y) < p_k \tag{2}$$

が得られる。

さらに

$$(1+ct) = \prod_{k \leq y}(1+kt)$$

から明らかに

$$1+ct \equiv 0 \pmod{1+kt}$$

となる。ゆえに

$$k \equiv -ckt \equiv -c(-1) \equiv c \pmod{1+kt}$$

したがって

$$k \equiv c \pmod{p_k}$$

ゆえに

$$F(x,\ y,\ k,\ z_{k1},\ \cdots,\ z_{km}) \equiv \begin{cases} F(x,\ y,\ c,\ a_1,\ \cdots,\ a_m) & \pmod{p_k} \\ 0 & \pmod{p_k} \end{cases}$$

ゆえに，(2)により

$$F(x,\ y,\ k,\ z_{k1},\ \cdots,\ z_{km}) = 0$$

がいえた。

つぎに，左辺を仮定して右辺を証明しよう。

まず，t と c とは

$$t = G(x,\ y)!, \qquad (1+ct) = \prod_{k \leq y}(1+kt)$$

によって定義する。

このとき

$$k,\ j \leq y, \qquad k \neq j \rightarrow (1+kt,\ 1+jt)=1$$

なることは，$1+kt$, $1+jt$ の公約数の中に素数があるとすれば $(k-j)t$ の約数の中の素数であり，$(k-j)|t$ が成立するから，この素数は t の約数となって

矛盾することから容易にわかる。

したがって，剰余定理により

$$a_i \equiv z_{ki} \qquad (\mathrm{mod}\ 1+kt),\ (k \leq y,\ i \leq m) \tag{3}$$

なる a_i が存在することが容易にわかる。いま，この $a_1, \cdots, a_m$ が右辺を満たすことを証明しよう。

前と同様に

$$c \equiv k \qquad (\mathrm{mod}\ 1+kt)$$

ゆえに

$$F(x, y, c, a_1, \cdots, a_m) \equiv \begin{cases} F(x, y, k, z_{k1}, \cdots, z_{km}) & (\mathrm{mod}\ 1+kt) \\ 0 & (\mathrm{mod}\ 1+kt) \end{cases}$$

となる。

$1+kt$ は互いに素であるから

$$\prod_{k \leq y} (1+kt) \mid F(x, y, c, a_1, \cdots, a_m)$$

ところで，(3)から

$$1+kt \mid a_i - z_{ki},\ z_{ki} \leq y$$

ゆえに

$$1+kt \mid \prod_{j \leq y} (a_i - j) \qquad (k \leq y)$$

ところで，$1+kt$ は互いに素であるから

$$\prod_{k \leq y} (1+kt) \mid \prod_{j \leq y} (a_i - j) \qquad (i \leq m)$$

これですべて証明された。

さて，補題を証明するためには，右辺が diophantine であることを確かめればよい。$u \mid v$ はもちろん $\exists w(uw = v)$ であるから，問題は $(1+ct)\prod_{j \leq y}(a_i - j)$ の形のところだけであり

$$\begin{aligned} &(1+ct) \mid \prod_{j \leq y} (a_i - j) \\ &\leftrightarrow a_i \leq y \lor \exists u \left(a_i > y \land (1+ct)u = \prod_{j \leq y} (a_i - y - 1 + j)\right) \end{aligned}$$

であるから，補題2により diophantine であることは明らかである。

われわれの重要な補助定理とは，補題3から明らかなつぎの定理である。

定理 1　$F(x, y, k, z_1, \cdots, z_m)$ を，有理整数を係数とする多項式とすれば

$$\exists y \forall k \leq y \exists z_1 \leq y \cdots \exists z_m \leq y (F(x, y, k, z_1, \cdots, z_m) = 0)$$

は diophantine である。

定理 2　すべての帰納的可算な命題は diophantine である。

[証明]　定理1と1·4節，定理2から明らかである。

第 3 章

群の語の問題

3·1 自由群

いま，Aを集合とするとき，Aの**語**を

$$a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1} \qquad (\text{ここに } a_i \in A \ (i=1, \cdots, n))$$

なる有限列と定義する。ここで，a_i^{+1} とは a_i 自身のことであり，a_i^{-1} というのは新しく導入された元であると思えばよい。nをこの語の**長さ**という。語の中には，$n=0$ すなわち空な列も入れて考える。空な列は表わしづらいので，ここでは e で表わすことにしよう。

Aの語について話を進めるときは，Aの元aおよび a^{-1} なる元をとくに**文字**とよぶことが多い。すなわち，語は文字の有限列のことである。文字bただ1個からなる語をふたたびbで表わすことにする。

いま，X, Yが2つの語であるとき，XとYとをつなぎ合わしてできた語を

$$XY$$

とかく。もう少し詳しくいえば，XとYとをそれぞれ

$$b_1 \cdots b_m, \ c_1 \cdots c_n$$

であるとすれば(ここに，$b_1, \cdots, b_m, c_1, \cdots, c_n$ はそれぞれ文字である)，XY は

$$b_1 \cdots b_m \ c_1 \cdots c_n$$

のことを表わすわけである。明らかなように，すべての語 X について

$$eX \quad \text{および} \quad Xe$$

は，X 自身を表わすわけである。

この記号法は，X，Y の2つの語だけではなく，$X_1, \cdots, X_k$ と有限個の語

についても成り立ち，このとき $X_1\cdots X_n$ は $X_1, \cdots, X_n$ をつなぎ合わせてできた語であると定義する。

例 X が $ab^{-1}c$, Y が $c^{-1}ab$, Z が $b^{-1}a^{-1}c$ ならば，XYZ は $ab^{-1}cc^{-1}abb^{-1}a^{-1}c$ である。

いま，Aの語について考えるとき，任意の文字bについてb^{-1}をつぎのように定義する。

b が $a\in A$ の形であるとき，b^{-1} は a^{-1} を意味する。b が a^{-1} $(a\in A)$ の形であるときは，b^{-1} はaを意味する。いま，語 X が $b_1\cdots b_n$ の形であるとき，X^{-1} を $b_n{}^{-1}\cdots b_1{}^{-1}$ と定義する。e^{-1} はe自身である。

Aの2つの語 X, Y が与えられたとき

$$X\overset{i}{=}Y$$

を，つぎの2つの条件

$$X \text{ は } Ubb^{-1}V \text{ で，} Y \text{ は } UV \text{ である} \tag{1}$$

$$X \text{ は } UV \text{ で，} Y \text{ は } Ubb^{-1}V \text{ である} \tag{2}$$

のいずれかを満たす語 U と V および文字bが存在することであるとする。

一般に，2つの語 X, Y が与えられたとき，$X=Y$ であるというのは，つぎの条件

$$X \text{ は } Z_1,\ Y \text{ は } Z_n \text{ であり，} Z_k\overset{i}{=}Z_{k+1}\ (k=1, \cdots, n-1) \text{ である}$$

を満たす

$$Z_1, \cdots, Z_n$$

が存在することをいう。ここに，$n=1$ でもかまわない。

このとき，つぎの性質は明らかであろう。

3·1·1 $X=X$

3·1·2 $X=Y\rightarrow Y=X$

3·1·3 $X=Y,\ Y=Z\rightarrow X=Z$

3·1·4 $eX=Xe=X$

3·1·5 $X^{-1}X=XX^{-1}=e$

3·1·6 $X=Y\rightarrow UXV=UYV$

3·1·7 Aの語全体に$X\cdot Y$をXYで定義すれば，e，$=$，$\cdot$，$^{-1}$に関して群をなす。この群をAの語がつくる**自由群**といって

$$[A]$$

によって表わす。

3·1·8 語$b_1\cdots b_i$が**標準形**であるというのは，いかなるk $(1\leq k<i)$をとってもb_kがb_{k+1}^{-1}でないことをいう。いま，Xを任意の語とするとき，$X=Y$で，Yが標準形であるようなYがただ一通り存在する。

[証明] 任意の語Xから出発して，(1)によってXを簡単にしてゆく変形を何度か行なえば，必ずXは標準形に還元することができる。

まず，(1)の方法をくり返して行なうことによってXを標準形に還元したとき，できあがるものがただ一通りであることを証明する。Xが

$$UWV$$

の形であるとき，WをXの**部分**という。ここに，UまたはVは空でもかまわない。Wが

$$a^{\pm1}\cdots a^{\pm1}$$

のように，すべて同じAの元の±1乗だけでできているとき，Wを**一様**であるという。Xの一様な部分で最大なものを**ブロック**という。Xを

$$B_1\cdots B_k$$

というブロックに分解する方法はただ一通りであることは明らかである。1つのブロックBが与えられて，$a^{i_1}\cdots a^{i_n}$であるとき

$$a^{i_1+\cdots+i_n}$$

なる形を導入して，これをBを計算してできた結果という。XとYとが2つの語であって，そのブロックへの分解がそれぞれ

$$B_1\cdots B_k \quad と \quad B_1'\cdots B_k'$$

であり，B_iとB_i'とを計算した結果が同じであるとき，XとYとをどのように(1)をくり返して標準形に還元しても，できあがったものが同じである，ということをkについての帰納法で証明する。

第1に，どのiをとってもB_iを計算した結果がa^0の形にならないときは，

X をどのように(1)で変形しても常に $B_1'' \cdots B_n''$ の形のブロックに分解されて，B_i'' を計算した結果は B_i と同じである。ゆえに，$B_2 \cdots B_n$ と $B_2' \cdots B_n'$ を考えることによって明らかである。

つぎに，たとえば B_i を計算した結果が a^0 の形であったとする。X, Y において，(1)をくり返して変形して標準形にもってゆく過程を

$$X=X_1,\ X_2,\ \cdots,\ X_n$$
$$Y=Y_1,\ Y_2,\ \cdots,\ Y_m$$

とする。このとき，$X_1, \cdots, X_n$ をずっとみてゆき，B_i に相当するところを全部消してゆくことにする。ただし，B_i に相当するところが別のブロックからきた元と打ち消し始めたら，B_i のブロックからきたものはすべてその別のブロックに属するものと考えることにする。同じようなことを B_i' に対しても行なって，できたものを

$$X'=X_1',\ X_2',\ \cdots,\ X_n'$$
$$Y'=Y_1',\ Y_2',\ \cdots,\ Y_n'$$

とすれば，この2つの系列のブロックの数はいずれも k より小さいから，数学的帰納法の仮定により

$$X_n'=Y_n'$$

が証明される。いま，$X_1, X_2, \cdots, X_n$ の系列で最初に消えてなくなるブロックを B_{i_0} とすれば，$i=i_0$ ととれば

$$X_n'=X_n$$

となるから，この議論によって

$$X_n=Y_m$$

がわかる。

つぎに，(2)の変形が用いられているときは，実際には

$$X=Ubb^{-1}VW,\quad UVW,\quad UVcc^{-1}W=Y$$

の場合に還元することができるが，この場合には $Ubb^{-1}Vcc^{-1}W$ という語から出発して，(1)を異なった順序で施したと考えることができるから，(1)だけを用いた場合に還元することができる。

3·1·9 G は群で，$A\subseteq G$ が G の生成元であるとき

$$h:[A]\to G$$

なる surjective (onto であること)な準同型 h が存在する。

[証明] $[A]$ の任意の語 $X=a_1^{\pm1}\cdots a_n^{\pm1}$ に対して

$$h(X)=a_1^{\pm1}\cdots a_n^{\pm1}$$

と定義する。ここに，右辺の $a_1^{\pm1}\cdots a_n^{\pm1}$ は，a_i が G の元として計算したものとする。このとき

$$X=Y\to h(X)=h(Y)$$

と h が surjective な準同型であることは明らかである。

3·1·10 G は群で，$\phi:A\to G$ とする。このとき

$$h:[A]\to G$$

なる準同型で，$a\in A$ に対しては $h(a)=\phi(a)$ なるものがただ一通り存在する。

[証明] A の語 $X=a_1^{i_1}\cdots a_n^{i_n}$ に対して，もしこのような h が存在すれば

$$h(X)=\phi(a_1)^{i_1}\cdots\phi(a_n)^{i_n}$$

となる。また，このように定義すれば h は準同型となる。

いま，G が群で $B\subseteq G$ であるとき，B から生成される G の部分群を $\{B\}$ とかくことにすれば，明らかである。

3·1·11 群 $[A]$ で $\{A\}$ は $[A]$ 自身である。すなわち，A は $[A]$ の生成元である。

3·1·12 $[A]\simeq[B]$ であるための必要十分な条件は $\bar{\bar{A}}=\bar{\bar{B}}$ である。

[証明] もし $[A]\simeq[B]$ ならば，$[A]$, $[B]$ の交換子群をそれぞれ G, H とすれば

$$[A]/G\simeq[B]/H$$

となる。ところで

$$[A]/G \quad \text{および} \quad [B]/H$$

は，それぞれ A, B を生成元とする**自由 Abel 群**である。したがって，$\bar{\bar{A}}=\bar{\bar{B}}$ がいえる。

逆に，$\bar{\bar{A}}=\bar{\bar{B}}$ ならば，$\phi: A \to B$ なる bijection (1対1で onto なこと)が存在する。したがって

$$h_1: [A] \to [B]$$
$$h_2: [B] \to [A]$$

で

$$h_1(a)=\phi(a) \qquad (a \in A)$$
$$h_2(b)=\phi^{-1}(b) \qquad (b \in B)$$

なる準同型が存在する。ところで

$$h_2 \cdot h_1: [A] \to [A]$$

は

$$h_2 \cdot h_1(a)=a \qquad (a \in A)$$

となるから，$h_2 \cdot h_1$ は恒等写像，同様に $h_1 \cdot h_2$ も恒等写像であるから，証明は終った。

ここで，$[A]$ の rank を $\bar{\bar{A}}$ によって定義する。自由群の rank は A のとり方によらず，その群としての構造だけで定まることが 3·1·12 によってわかる。

いま G が群で，$A \subseteq G$ とする。このとき，A が G の中で**自由**であるということは

$$h: [A] \to G$$

で

$$h(a)=a \qquad (a \in A)$$

なる準同型 h が injective (1対1のこと)であることをいう。このとき，G の部分群 $\{A\}$ と $[A]$ とは同型であるので，$\{A\}$ のことをしばしば $[A]$ とかく。

$A \cap B=\phi$ のとき，$[A \cup B]$ であることを

$$[A, B]$$

とかく。$[A, B]$ とかいたときは必ず $A \cap B=\phi$ とする。もし $A \cap B=\phi$ でないときは，B のコピーの中で A と共通部分のないものを，あらためて B とおき直したものについて常に $A \cap B=\phi$ を仮定するものとする。$[A, B, C]$ なども同様にして定義する。B が z だけからなる集合 $\{z\}$ であるとき，$[A, B]$ のことを $[A, z]$ とかくことにする。

3·1·13 自由群 $[A, z]$ において

$$S=\{XzX^{-1}|X\in[A]\}$$

とすれば，S は $[A, z]$ で自由である。

[証明] いま

$$W=(X_1zX_1^{-1})^{i_1}\cdots(X_nzX_n^{-1})^{i_n} \qquad (i, j=\pm1)$$

として，W が(1)の変形だけで e に還元されたとする。もし $n>0$ のときは，この変形で z および z^{-1} のゆくえを追ってゆくことにする。もし zz^{-1} および $z^{-1}z$ を e に還元する変形が行なわれたとすれば，それは全体として

$$XzX^{-1}(YzY^{-1})^{-1}=XzX^{-1}Yz^{-1}Y=Xzz^{-1}Y=XY$$

に相当する変形が行なわれたにちがいない。したがって，$X=Y$ でなければならない。したがって，このときわれわれは単に

$$(XzX^{-1})(XzX^{-1})^{-1}=e \qquad (3)$$

なる変形を行なうことにする。けっきょく，W は(3)の変形によって e に還元されることがわかるから，S は自由である。

3·2 関係のある群

Aについての関係とは，$X=Y$ なる式を意味する。ここに，X, Y はAの語であるものとする。

いま，K を $[A]$ の正規部分群とするとき，$X=Y$ が因子群 $[A]/K$ で成立しているとは，X と Y とが K の同じ剰余類に属していることと定義する。いいかえれば，$XY^{-1}\in K$ のときに成立している。

いま，RをAについての関係の集合であるとする。このとき，Aについてのある関係が R から導かれるというのは，R の関係をすべて満たす $[A]$ の因子群において，この関係が成立していることを意味する。Rから導かれる関係全体の集合を $C(R)$ で表わすことにする。いま，Rの関係 $X=Y$ から XY^{-1} をつくって，このようなすべての XY^{-1} から生成される $[A]$ の正規部分群を K_R とすれば，$[A]/K_R$ で成立する関係の全体はちょうど $C(R)$ と一致する。われわれは $[A]/K_R$ のことを，Aを生成元としてRによって定義される群とよんで

$$[A;\ R]$$

とかくことにする。または，生成元 A と関係 R をもっている群ともいう。

われわれは $[A; R]$ の記号を広く用いることにする。たとえば，$[A, B;\ R, S]$ というのは

$$[A\cup B;\ R\cup S]$$

のことで，ここに以前と同じく $A\cap B=\phi$ を仮定することにする。また，$[A, t;\ R, X=Y]$ は

$$[A\cup\{t\};\ R\cup\{X=Y\}]$$

のことである。さらに，$[\quad]$ の内部で；の前に A があって a が；のあとにあるときは，A のすべての元 a について考えるという意味であるとする。たとえば，$[A, t;\ at=ta]$ は

$$[A,\ t;\ \{at=ta\,|\,a\in A\}]$$

の意味であり，$[A, B;\ ab=ba]$ は

$$[A,\ B;\ \{ab=ba\,|\,a\in A\wedge b\in B\}]$$

の意味である。

さらに，われわれは大胆な用法を使用することにしよう。G が群であるとき，**3・1・9** により $h:[G]\to G$ なる surjective な準同型がある。いま，XY^{-1} が h の核にはいるような関係 $X=Y$ 全体の集合を R_G として，上のように K_R をつくれば

$$G\simeq[G]/K_R$$

すなわち

$$G\simeq[G;\ R_G]$$

となる。以下，G と $[G; R_G]$ とを同一視することにする。$G, H, \cdots$ が群であるとき

$$[G,\ H,\ \cdots;\ R]$$

を考えるというときには，常に

$$[G,\ H,\ \cdots;\ R_G\cup R_H\cup\cdots\cup R]$$

を考えるものとする。もちろん，$G, H, \cdots$ の中で群でないものについては何

もつけ加えないものとする。したがってこの記号法を用いれば，G, H が群であるときに，$G\times H$ は

$$[G, H;\ gh=hg]$$

によって表わされることになる。

3·3 融 合 積

H, H' はそれぞれ群 G, G' の部分群で，$\phi: H\to H'$ は H から H' の上への同形対応であるとする。このとき，G, G' の ϕ による**融合積**というのは

$$[G, G';\ h=\phi(h)]$$

なる群のことと定義して

$$G *_\phi G'$$

によって表わす。

$H=H'$ なる部分を**融合部分**という。

いま，G の部分群 H のすべての左剰余類(ただし H 自身は除く)から1つだけ代表元をとり出して，その全体の集合を T とする。同様に，G' の部分群 H' のすべての左剰余類(ただし H' 自身は除く)から1つだけ代表元をとり出して，その全体の集合を T' とする。

このとき，$G\cup G'$ の語が**正規**であるとは，その語が

$$t_1 \cdots t_n h$$

の形であって，$h\in H$, t_1, $\cdots$, $t_n \in T\cup T'$ で，t_i と t_{i+1} は一方が T に属し他方は必ず T' に属していなければならないという条件が満たされているものとする。すなわち

$$t_i \in T \leftrightarrow t_{i+1} \in T'$$

が成立する。

この状況において，つぎの定理が成立する。

定理 1 $G *_\phi G'$ の任意の元は正規な語によって表わされる。しかも，正規な語に表わす方法はただ一通りである。

[証明] $G *_\phi G'$ の任意の元は

$$g_1 \cdots g_n h$$

の形で表わされる。ここに，$h \in H$ で $g_1, \cdots, g_n \in (G \cup G' - H)$ であり，g_i, g_{i+1} は，一方が G に属し他方は必ず G' に属していなければならないものとする。いま，$T \cup T'$ から $\bar{g}_1, \cdots, \bar{g}_n$ をとり出して

$$g_i = \bar{g}_i h_i, \qquad h_i \in H$$

とすることができる。すなわち，もともとの元は，つぎの形となる。

$$\bar{g}_1 h_1 \bar{g}_2 h_2 \cdots \bar{g}_n h_n h \tag{1}$$

ところで，一般に $h' \in H$, $\bar{g} \in T \cup T'$ が与えられたときは

$$h'\bar{g} = \bar{g}'h'', \qquad \bar{g}' \in T \cup T', \qquad h'' \in H$$

なる $\bar{g}'$ がただ一通りに定まるから，(1)において h を順々に左から右へ移してゆくことができて，上の形から

$$\bar{g}_1 \bar{g}_2' \cdots \bar{g}_n' h_0$$

なる正規な語がここに述べた方法でただ一通りに定まる。いま，ここに述べた方法で $g_1 \cdots g_n h$ から得られた正規な語を $F(g_1 \cdots g_n h)$ と表わすことにしよう。われわれはこの F を用いて，正規な語に表わす方法がただ一通りであることを証明しようというのである。

いま，M を正規な語全体の集合としよう。ここで，M の2つの元が等しいということは，正規に表わした表わし方が等しいということである($G *_\phi G'$ の元として等しくても，表現が異なれば異なっているものとする)。

$g \in G \cup G'$ とするとき

$$|g| : M \to M$$

なる $|g|$ を

$$|g|(\bar{g}_1 \bar{g}_2 \cdots \bar{g}_n h) = F(g \bar{g}_1 \bar{g}_2 \cdots \bar{g}_n h)$$

と定義する($g, \bar{g}_1 \in G$, $g, \bar{g}_1 \in G'$, $g \in H \cup H'$ の3つの場合については，F の定義を上に述べたことより少し拡張しなければならないが，その拡張は自明であるから省略する)。

明らかに $|e|$ は M の上の恒等写像になっている。

さらに，$g, g' \in G \cup G'$ とするとき，いろいろな場合に分けて考えることに

よって，容易に

$$|g|\cdot|g'|=|gg'|$$

であることがわかる(詳細は演習問題として証明されたい。g, g' の一方が $H\cup H'$ にはいっている場合，両方とも同じ $G-H$，または $G'-H'$ にはいっている場合，異なったほうにはいっている場合，g' と $\bar{g}_1$ とが同じ $G-H$ または $G'-H'$ にはいっている場合，異なったほうにはいっている場合，などに分ければよい)。

以上の2つから

$$|g^{-1}|=|g|^{-1}$$

であることがわかり，したがって $|g|$ が M の置換群の元であることがわかる。いま，M の置換群を S_M で表わすことにしよう。明らかに $g\to|g|$ は，$g\in G$ なる g だけをとれば G から S_M への準同型であり，$g\in G'$ なる g だけをとれば G' から S_M への準同型になっている。$g\neq e$ $(g\in G\cup G')$ とすれば，$|g|(e)=\bar{g}h$ で $g=\bar{g}h$ $(g\in G)$ または $g=\bar{g}\phi(h)$ $(g\in G')$ となるから，いずれにしても $|g|\neq e$ となって，これはそれぞれ G から S_M の中への同型写像および G' から S_M への同型写像となっている。したがって，S_M の中で G と G' とに同型な部分群が存在する。この部分群のことをまた G, G' とかくことにする。この同型写像は容易に

$$[G, G'; R_G, R_{G'}]\to S_M$$

なる準同型写像に拡散することができる($[G, G']\to S_M$ をつくって，その核の中に ${}^K R_G$, ${}^K R_{G'}$ がはいっていることをみればよい)。

この準同型写像の核の中に $h^{-1}\phi(h)$ がはいっていることは明らかであるから，この写像から

$$G*_\phi G'\to S_M$$

なる準同型写像が得られ，S_M の中の $G\cup G'$ はこの準同型の像に含まれることがわかる。この準同型を φ とかくことにしよう。

$$\varphi: G*_\phi G'\to S_M$$

さて，$G*_\phi G'$ の元が $\bar{g}_1\cdots\bar{g}_n h$ と $\bar{g}_1'\cdots\bar{g}_n' h'$ との2つの正規な形に表

わされたとすれば

$$\varphi(\bar{g}_1\cdots\bar{g}_nh)=|\bar{g}_1|\cdots|\bar{g}_n||h|$$
$$\varphi(\bar{g}_1'\cdots\bar{g}_m'h)=|\bar{g}_1'|\cdots|\bar{g}_m'||h|$$

で，これを e に施せば，それぞれ $\bar{g}_1\cdots\bar{g}_nh$ と $\bar{g}_1'\cdots\bar{g}_m'h'$ を得るから，もし $\bar{g}_1\cdots\bar{g}_nh=\bar{g}_1'\cdots\bar{g}_m'h'$ が $G*_\phi G'$ で成立すれば，正規な語としてもまったく同じでなければならない。すなわち，$n=m$, $\bar{g}_1=\bar{g}_1'$, …, $\bar{g}_n=\bar{g}_n'$, $h=h'$ がわかって，証明が終った。

系 Gの元と，それ自身によって表わされる $G*_\phi G'$ の元との対応は injective である。したがって，$G*_\phi G'$ は G 自身を含んでいると考えられる。これをふたたび G で表わすことにする。G' についても同様のことをすれば，この $G*_\phi G'$ の中の G, G' について，つぎの式が成立する。

$$\{G, G'\}=G*_\phi G', \qquad G\cap G'=H=H'$$

さて，G, G', H, H', ϕ は上のとおりとする。いま，K, K' はそれぞれ G, G' の部分群であって

$$\phi(H\cap K)=H'\cap K'$$

が満たされているものとする。いま，ϕ を $H\cap K$ に制限してできる関数を，あらためてψとかくことにする。集合論などで用いられる記号を用いれば

$$\psi=\phi\restriction H\cap K$$

である。

$$\psi: H\cap K\to H'\cap K'$$

が同型写像であることは明らかであろう。したがって，$K*_\psi K'$ をつくることができる。$K*_\psi K'$ の元にそれ自身で表わされる $G*_\phi G'$ の元を対応させることによって，$K*_\psi K'$ から $G*_\phi G'$ への準同型χが定義される。χの像は $\{K, K'\}$ となる。この状況において，つぎの性質が成立する。

3·3·1 χ は injective である。

［証明］ K の中の $H\cap K$ の異なった左剰余類は，Gの中の H の異なった左剰余類に属するから，定理1の T を選ぶときに，もし K の元がその剰余類の

中に存在するときには代表元を K の元の中から選ぶようにする。そうすると，$T\cap K$ が K と $H\cap K$ とについて選ばれた剰余類の代表の集合となる。同じことを T' についても仮定する。このとき，$K\cap K'$ の語で正規なものは，$G\cup G'$ の語と考えてみても正規になっている。したがって，定理 1 によって χ が injective なことは明らかである。

3·3·1 によって，$K*_{\phi}K'$ を今後 $G*_{\phi}G'$ の中の $\{K, K'\}$ と同一視することにする。このとき，つぎの性質が成立する。

3·3·2 $$G\cap\{K, K'\}=K$$

ここで，すべての群は $G*_{\phi}G'$ の中で考えられているとする。

[証明] = の左辺が右辺に含まれることをいえば十分である。3·3·1 の場合と同じように T をとれば，G の任意の元の正規な語の表現は th である。この表現が $\{K, K'\}$ の元の正規な表現であるためには，$t\in T\cap K$, $h\in K\cap H$ でなければならない。すなわち，$th\in K$ で，証明は終った。

$G*_{\phi}G'$ の特別な場合として，H と H' とが単位元だけからなる部分群の場合に，この群を単に

$$G*G'$$

とかいて，G と G' との**自由積**とよぶ。

したがって

$$G*G'=[G, G']$$

とかいてよい。ここで，$[G, G']$ は以前の約束を用いたかき方で，詳しくかけば

$$[G, G', R_G, R_{G'}]$$

のことである。いま K, K' をそれぞれ G, G' の任意の部分群とすれば，この特別な場合にはいつでも 3·3·1，3·3·2 が成立している。すなわち，$K*K'$ は $G*G'$ の部分群と考えてよく，$G*G'$ の中で $G\cap K*K'=K$ が成立している。

さて，G, G' がもっと大きな群 L の中の部分群である場合を考えよう。いま，$H=G\cap G'$ として，ϕ を H から H への恒等写像とする。このとき

$$G *_{\phi} G' \to L$$

なる準同型が定義される。この準同型が injective である場合には，われわれは $G *_{\phi} G'$ を L の中の $\{G, G'\}$ であると思ってもよい。このことが成立するとき，われわれは $\{G, G'\}$ を G と G' の H による**融合積**であるという。とくに H が e だけからなるときは，単に G と G' の自由積であるという。

3·3·3　$e \neq h \in H$ とならば，$G * H$ において $\{G, hGh^{-1}\}$ は G と hGh^{-1} の自由積である。

［証明］　定理1により，$G \cap hGh^{-1} = \{e\}$ であることは明らかである。つぎに，$\{G, hGh^{-1}\}$ の任意の元を $G * hGh^{-1}$ の元として正規に表現して

$$a_1 \cdot a_2 \cdots a_n \qquad (2)$$

とする。すなわち

$$a_i \in G \leftrightarrow a_{i\pm 1} \in hGh^{-1}$$

が成立するようにおく。

もし $a_1 \cdots a_n$ が $\bar{e}$ とは異なる表現であれば，その中の $a_i \in hGh^{-1}$ をすべて hg_ih^{-1} なる形にかえて(2)をかき直せば，こうしてかき直された表現自身が $G * H$ の元の表現として正規である。したがって，e ではない。よって証明された。

3·4　有限表示群

群 G が $[A; R]$ で表わされるとき，$[A; R]$ を G の**表示**という。いま，A も R もともに有限であるとき，G は有限の表示 $[A; R]$ をもつといい，G を**有限表示群**であるという。

3·4·1　G_1, G_2 が有限表示群ならば，$G_1 \times G_2$ も有限表示群である。

［証明］　$[A; R] \times [B; S] = [A, B; R, S, ab = ba]$

ここで，a, b の動く範囲が A と B，すなわち有限であることに注意せよ。

3·4·2　いま，$G *_{\phi} G'$ が $\phi: H \to H'$ で $H \subseteq G$, $H' \subseteq G'$ なる状況でつくられたとして，G, G' が有限表示群で，H が有限個の生成元をもてば $G *_{\phi} G'$ も有限表示群である。

[証明] G, G' の有限表示をそれぞれ $[A;R]$, $[B;S]$ として, H の有限個の生成元を $h_1, \cdots, h_n$ とする。$h_1, \cdots, h_n$ を A の語として表わした表現を $X_1, \cdots, X_n$ とし, $\phi(h_1), \cdots, \phi(h_n)$ を B の語として表わしたものを $Y_1, \cdots, Y_n$ とすれば

$$G *_\phi G' = [A, B; R, S, X_1 = Y_1, \cdots, X_n = Y_n]$$

となるからよい。

Aを有限として, RがAの関係の集合であるとする。このとき, $[A;R]$ の語の問題というのは, 任意に与えられたAの関係 $X=Y$ が R から導かれるかどうかを決定することをいう。いいかえれば, $X=Y$ が $C(R)$ に属するかどうかを決定することである。すなわち, $X=Y$ が $[A;R]$ で成立するかどうかを決めることである。

$[A, R]$ の語の問題を effective に解くということを定義しよう。

いま, Aを有限として, その元を $a_1, \cdots, a_n$ としよう。この $a_1, \cdots, a_n$, $a_1^{-1}, \cdots, a_n^{-1}$, $=$ に, それぞれ適当に自然数を対応させれば, Aの語 X, 関係 $X=Y$ などはすべて自然数の有限列と考えられるから, そのゲーデル数が対応させられる。

X や $X=Y$ のゲーデル数を「X˥, 「$X=Y$˥ で表わすことにしよう。$[A;R]$ の語の問題が effective に解けるということは, $X=Y$ が与えられたとき, $X=Y$ が R から導かれるかどうかを effective に決定する方法をみいだすことをいう。もう少し別な言葉でいえば, 自然数の上の帰納的な関係 f を与えて

$$f(\ulcorner X=Y \urcorner)=0 \leftrightarrow \text{‘}X=Y \text{ は } R \text{ から導かれる’}$$

が成立するようにできるということである。この f を求めることを, 語の問題の effective な解法をみつけるということである。

この effective という性質が $a_1, \cdots, a_n$, ϕ, $a_1^{-1}, \cdots, a_n^{-1}$, $=$ に相異なる自然数を対応させる, 対応のさせ方に無関係であることは帰納的であるということの性質から明らかであろう。

いま，語の問題の effective な解法があったとする。このとき

$$(X=Y)\in C(R)\leftrightarrow \text{‘}X=Y \text{ は } A \text{ の関係である’} \wedge f(\ulcorner X=Y\urcorner)=0$$

が成立する。ところで，Aは有限であるから‘$X=Y$ はAの関係である’はもちろん「$X=Y$⌉についての帰納的な命題である。ゆえに，$C(R)$ は「$X=Y$⌉についての帰納的な命題であると思ってよい。

逆に，$C(R)$ が「$X=Y$⌉についての帰納的な命題であれば

$$(X=Y)\in C(R)\leftrightarrow f(\ulcorner X=Y\urcorner)=0$$

を満たす帰納的な関数fが存在する。このfは明らかに［A; R］の effective な語の問題の解法になっている。

したがって，［A; R］の語の問題を effective に解けるかどうかは，$C(R)$ が帰納的な集合になっているかどうかということと同等である。

本章の目的は，つぎの定理である。

定理 2（Novikoff–Boone の定理） 有限表示群［A; R］で，その語の問題が effective に解けないものがある。

この定理は Novikoff によって，またそれから少し遅れて独立に Boone によって得られたものである。この章では，その後 Higman によって得られた定理を証明して，その系としてこの定理を証明することにする。

3・5 Higman 群

群 H を群 G に**うめこめる**ということは

$$h: H\to G$$

なる H から G の中への同型写像が存在することをいう。

群 G が **Higman 群**であるというのは，G に有限個の生成元が存在して，その上 G がある有限表示群の中にうめこめることをいう。この節では，Higman 群の基本的な性質について調べることにする。

3・5・1 G, H が Higman 群ならば

$$G\times H$$

も Higman 群である。

[証明] $G\times H$ が有限個の生成元をもつことは明らかである。いま，G, H がそれぞれ有限表示群 L, M にうめこめるとすれば，$G\times H$ は明らかに有限表示群 $L\times M$ にうめこめるからよい。

3·5·2 G, G' が Higman 群であり，H, H' はそれぞれ G, G' の部分群であるとする。$\phi: H\to H'$ は同型写像で，H が有限個の生成元をもてば

$$G *_{\phi} G'$$

も Higman 群である。

[証明] $G *_{\phi} G'$ が有限個の生成元をもつことは明らかである。いま，$G\subseteq\tilde{G}$, $G'\subseteq\tilde{G}'$ で $\tilde{G}$, $\tilde{G}'$ が有限表示群とすれば，$G *_{\phi} G'$ は $\tilde{G} *_{\phi} \tilde{G}'$ の部分群であり，後者は 3·4·2 により有限表示群であるからよい。

さて，ϕ が群 G の中の同型写像であるというのは，ϕ が G のある部分群 H から G の中への同型写像になっていることをいう。

このような G の中の同型写像 ϕ に対して，G_ϕ をつぎの式で定義する。

$$G_\phi=[G, t;\ tht^{-1}=\phi(h)]$$

ここで，h は H のすべての元を走るものとする。

G_ϕ のいろいろな性質を調べよう。まず準備として，$[G, r]$ についての性質から始めることにしよう。

3·5·3 Hを群Gの部分群とすれば，群 $[G, r]=G*[r]$ の中で $\{G, rHr^{-1}\}$ はGと rHr^{-1} の自由積である。

[証明] 3·3·3 により，$\{G, rGr^{-1}\}$ はGと rGr^{-1} の自由積である。ゆえに，3·5·3 は 3·3·1 から出てくる。

3·5·4 ϕ は G の中の同型写像で，H の上で定義されているとする。G と同型な群 G_1 をとり，G から G_1 への同型写像を $g\mapsto g_1$ とする。このとき $[G, r]$ の部分群 $\{G, rHr^{-1}\}$ から $[G_1, s]$ の部分群 $\{G_1, s\phi(H)s^{-1}\}$ への同型写像 ψ を

$$\psi(g)=g_1, \qquad \psi(rhr^{-1})=s\phi(h)s^{-1}$$

によって定義すれば，つぎの関係が成立する。

$$[G, r] *_\phi [G_1, s] = G_\phi * [s]$$

[証明]　$[G, r] *_\phi [G_1, s] = [G, G_1, r, s;\ g = g_1,\ rhr^{-1} = s\phi(h)s^{-1}]$

$$= [G, r, s;\ rhr^{-1} = s\phi(h)s^{-1}]$$

$$= [G, r, s, t;\ rhr^{-1} = s\phi(h)s^{-1},\ t = s^{-1}r]$$

$$= [G, t, s, r;\ tht^{-1} = \phi(h),\ r = st]$$

$$= [G, t, s;\ tht^{-1} = \phi(h)] = G_\phi * [s]$$

3・5・5　Gの元を自分自身で表わす元に対応させる対応は，G から G_ϕ の中への同型写像である。

[証明]　3・5・4 の証明から明らかである。

この性質によって，今後Gを G_ϕ の部分群と考えることにする。そのとき，$\phi(h) = tht^{-1}$ によってϕは完全に t で表わされる。

この状況において，つぎの性質が成立する。

3・5・6
$$G \cap t^{-1}Gt = H$$

[証明]　3・3・3 により，$\{G, rGr^{-1}\}$ はGと rGr^{-1} との自由積であるから，3・3・1 により

$$\{G, rHr^{-1}\} \cap rGr^{-1} = rHr^{-1}$$

となる。同様にして

$$\{G_1, s\phi(H)_1 s^{-1}\} \cap sG_1 s^{-1} = s\phi(H)_1 s^{-1}$$

したがって，3・3・1 により $rGr^{-1} *_\phi sG_1 s^{-1}$ は $[G, r] *_\phi [G_1, s]$ の部分群と考えてよく，$\{rGr^{-1}, sG_1 s^{-1}\}$ となる。さらに，つぎのことが成立する。

$$\{rGr^{-1}, sG_1 s^{-1}\} = \{rGr^{-1}, sGs^{-1}\}$$

$r^{-1}s = t^{-1}$ であるから，$rGr^{-1} *_\phi sG_1 s^{-1} = \{rGr^{-1}, sGs^{-1}\}$ に r^{-1} による内部同型を適応すれば

$$G *_\phi t^{-1}G_1 t = \{G, t^{-1}Gt\}$$

であり，ここに

$$\{G, t^{-1}Gt\} = [G, t^{-1}Gt;\ tht^{-1} = h]$$

で表わされる。すなわち，これはGと $t^{-1}Gt$ との H による融合積であることがわかる。ゆえに

$$G\cap t^{-1}Gt=H$$

が得られる。

さて，G, ϕ, H はいままでどおりとする。このとき，G の部分群 K が ϕ で不変であるということを，条件

$$\phi(H\cap K)=\phi(H)\cap K$$

で定義する。

もし K が ϕ で不変であれば，$\phi\restriction K$ は K の中の同型写像である。いま，この同型写像を ϕ' とおこう。

この状況で，つぎの性質が成立する。

3·5·7 $K_{\phi'}$ の元にそれ自身で表わされる元を対応させる写像は，$K_{\phi'}$ から G_ϕ へのうめこみである。すなわち，$K_{\phi'}$ は G_ϕ の部分群と思ってよい。

[証明] G_ϕ を前のように $[G, r]*_\phi[G_1, s]$ の中にうめこんで考える。ϕ' から同様に ψ' をつくって $[K, r]*_{\psi'}[K_1, s]$ をつくれば，$K_{\phi'}$ はこの中にうめこめるから，$[K, r]*_{\psi'}[K_1, s]$ が $[G, r]*_\psi[G_1, s]$ の中にうめこめることをいえばよい。

$[K, r]$, $[K_1, s]$ はそれぞれ $[G, r]$, $[G_1, s]$ の部分群であるから，3·3·1 により $\{K_1, r\}$ と $[G, r]*_\phi[G_1, s]$ の融合部分との共通部分が $\{K_1, s\}$ と $[G, r]*_\phi[G_1, s]$ の融合部分との共通部分に等しいことを証明すれば十分である。

まず，つぎの式を証明しよう。

$$\{K, r\}\cap\{G, rHr^{-1}\}=\{K, r(H\cap K)r^{-1}\} \qquad (1)$$

まず，$\{G, rHr^{-1}\}$ は自由積となるから，その元の正規表現は

$$\cdots g_1rh_1r^{-1}g_2rh_2r^{-2}\cdots$$

となっている。この形が $\{K, r\}=[K, r]$ の中にはいるためには，g_i, h_i がすべて K にはいることが必要十分である。すなわち，(1)が得られた。

同様にして，つぎの式が得られる。

$$\{K_1, s\}\cap\{G_1, s\phi(H)_1s^{-1}\}=\{K_1, s(\phi(H)_1\cap K_1)s^{-1}\} \qquad (2)$$

ところで，$\phi(H\cap K)=\phi(H)\cap K$ であるから，(1), (2)の右辺はちょうど ψ に

よって対応しているものであり，求めるつぎの式が得られた。

$$\{K, r\}\cap\{G, rHr^{-1}\}=\{K_1, s\}\cap\{G_1, s\phi(H)_1 s^{-1}\}$$

3·5·7 により，$K_{\phi'}$ を G_ϕ の $\{K, t\}$ なる部分群と思ってよい。こうした上で，つぎの性質が成立する。

3·5·8 $$\{K, r, s\}\cap\{G, r\}=\{K, r\}$$

[証明] 3·3·2 より明らかである。

3·5·9 $$\{K, r\}\cap G=K$$

[証明] 3·3·2 を $\{K, r\}=K*[r]$ にあてはめれば明らかである。

3·5·10 $$\{K, t\}\cap G=K$$

[証明] 3·5·8 と 3·5·9 より，$\{K, r, s\}\cap G=K$ となるから明らかである。

さて，ϕ, ψ, $\cdots$ がすべて G の中の同型写像であるとする。このとき

$$G_{\phi,\psi,\dots}=[G, t_\phi, t_\psi, \cdots; t_\phi h t_\phi^{-1}=\phi(h), \cdots]$$

としよう。

3·5·11 G は $G_{\phi,\psi,\dots}$ の中にうめこまれている。すなわち，G を $G_{\phi,\psi,\dots}$ の部分群であると思ってよい。

[証明] もしGの相異なる元 g, g' が，$G_{\phi,\psi,\dots}$ の中で $g=g'$ となったとすれば，$g=g'$ は $G_{\phi,\psi,\dots}$ の中の有限個の関係から導かれなければならない。したがって，$G_{\phi_1\cdots\phi_n}$ という有限個の $\phi_1\cdots\phi_n$ で，すでに $g=g'$ となっている。ところで

$$G_{\phi_1\cdots\phi_n\phi_{n+1}}=(G_{\phi_1\cdots\phi_n})_{\phi_{n+1}}$$

であるから，3·5·5 に反する。

3·5·12 K は G の部分群で，すべての ϕ, ψ, $\cdots$ に対して不変であるとする。このとき，つぎの式が成り立つ。

$$\{K, t_\phi, t_\psi, \cdots\}\cap G=K$$

[証明] $\{K, t_\phi, t_\psi, \cdots\}$ のすべての元は，有限個の $t_{\phi_1}, \cdots, t_{\phi_n}$ をとれば $\{K, t_{\phi_1}, t_{\phi_2}, \cdots, t_{\phi_n}\}$ の中にはいっている。したがって，3·5·10 を何度か用いることによって容易に証明される。

3·6 benign について

benign はビナインと読む。辞書を引くと‘慈悲ぶかい，親切な；温和な［気候など］；［医］良性の’と訳が出ている。以下の感じは‘［医］良性の’に相当すると思うので，もう少し説明することにする。腫瘍で悪性のものはガンのようなもので，生命とりでどうにもならないものである。しかし，腫瘍で悪性でないものは，その場所があまりふくれ上がると骨や神経を圧迫して困るがそれ以外はたいしたことはなく，手術でとるのも簡単というものがある。こういう腫瘍を benign な腫瘍というのである。したがって，以下は面倒な腫瘍をとり去る外科医のつもりで，どのようなものが benign であるかを調べてゆくことにする。

まず，順々に定義をしてゆくことにして，いま H は G の部分群で，ϕ が H から H への恒等写像であるとき，G_ϕ のことを G_H とかくことにする。

いま，ϕ を H の恒等写像とすれば，G の任意の部分群 K について，K は ϕ で不変であるから，$H_{H\cap K}$ は G_H の部分群であると思ってよい。

さて，G が Higman 群であったとする。G の中の同型写像 ϕ が benign であるということを，G_ϕ が Higman 群であること，と定義する。G の部分群 H が benign であるというのは，G_H が Higman 群になることをいう。

G は有限個の生成元をもつから，G_ϕ も G_H も有限個の生成元をもつことは明らかであるが，このことは以下断りなしに用いることにする。

3·6·1　G が Higman 群で，ϕ が G の有限個の生成元をもつ部分群 H からの同型写像(G の中への)ならば，ϕ は G の中で benign である。

［証明］　3·5·2 により，$[G, r]$ と $[G_1, s]$ とは Higman 群である。

$\{G, rHr^{-1}\}$ は有限個の生成元をもつから，ふたたび 3·5·2 により $[G, r] *_\phi [G_1, s]$ も Higman 群である。したがって，G_ϕ は Higman 群の部分群で，有限個の生成元をもつから，やはり Higman 群である。

3·6·2　H が Higman 群 G の部分群で，有限個の生成元をもてば，H は G で benign である。

［証明］　3·6·1 から明らかである。

3·6·3 Lが Higman 群で，GはLの部分群でやはり Higman 群であるとする。そのとき，Gの中の同型写像ϕがGで benign であることとLで benign であることは同等である。したがって，G の部分群 H が G で benign であることとLで benign であることもやはり同等である。

［証明］ いま，L_ϕ が Higman 群であるとすれば，G_ϕ は L_ϕ の部分群で有限個の生成元をもつから，やはり Higman 群である。

さて今度は，逆に G_ϕ が Higman 群であると仮定しよう。L と同型な L のコピーを1つつくって，それを L_1 として，Lの元aに対応する L_1 の元を a_1 で表わすことにしよう。このとき，Gの上でϕを

$$\phi(g)=g_1$$

で定義すれば，3·5·2 により $G_\phi *_\phi K_1$ は Higman 群である。いま，ϕの定義域を H とおけば

$$\begin{aligned}G_\phi *_\phi K_1&=[G,\ t,\ K_1;\ tht^{-1}=\phi(h),\ g=g_1]\\&=[G,\ t,\ K_1;\ th_1t^{-1}=\phi(h)_1,\ g=g_1]\\&=[K_1,\ t;\ th_1t^{-1}=\phi(h)_1]\simeq K_\phi\end{aligned}$$

となるから，K_ϕ も Higman 群である。

この 3·6·3 により，われわれはϕまたはHが benign であるというとき，どの Higman 群の中で考えているかということを述べる必要がないことがわかる。したがって，以下ではそのことにふれないで議論を進める。

3·6·4 H と K とが benign な部分群ならば，$H\cap K$ と $\{H,K\}$ もともに benign である。以下，H, K は Higman 群 G の部分群とする。

［証明］ 最初に K が有限個の生成元をもっている(したがって，Higman 群である)ことを仮定して証明をする。

このとき，$K_{H\cap K}$ は G_H の部分群である。したがって，$H\cap K$ は benign である。

$\{H,K\}$ については，G_H で $\{G,t^{-1}Gt\}$ は G と $t^{-1}Gt$ とについての H と $t^{-1}Ht$ とを同一視してできる融合積である。ところで，$\{H,K\}$ も $t^{-1}Gt$ も，この融合部分を含んでいるので，3·3·2 により

$$\{H, K, t^{-1}Gt\} \cap G = \{H, K\} \tag{1}$$

したがって

$$\{K, t^{-1}Gt\} \cap G = \{H, K\}$$

が得られる。

ところで，左辺の2つの群はともに有限の生成元をもつので，その共通部分は benign である。

さて一般の場合は，G_H において

$$G \cap t^{-1}Gt = H$$

であるから

$$H \cap K = G \cap (t^{-1}Gt \cap K)$$

となる。

ところで，G も $t^{-1}Gt$ も有限個の生成元をもつから，上に証明した特殊な場合を2度用いることにより，$H \cap K$ が benign であることがわかる。

(1)は一般の場合にも成立しているから，G が有限個の生成元をもつことから $\{K, t^{-1}Gt\}$ が benign であることがわかり，$\{H, K\}$ も benign であることがわかる。

3·6·5 G_1, G_2 が Higman 群であって，$\phi : G_1 \to G_2$ は準同型とする。このとき，H_1 が G_1 の benign な部分群であれば $\phi(H_1)$ は G_2 の benign な部分群であり，逆に H_2 が G_2 の benign な部分群であれば $\phi^{-1}(H_2)$ は G_1 の benign な部分群である。

[証明] 3·5·1 によって，$G_1 \times G_2$ は Higman 群である。Q を $(g_1, \phi(g_1))$ なる形の $G_1 \times G_2$ の部分群であるとする。もちろん $Q \simeq Q_1$ となる。

したがって，G_1, G_2, Q はすべて $G_1 \times G_2$ の部分群で，有限の生成元をもつので benign である。ゆえに

$$\phi(H_1) = \{\{H_1, G_2\} \cap Q, G_1\} \cap G_2$$
$$\phi^{-1}(H_2) = \{\{H_2, G_1\} \cap Q, G_2\} \cap G_1$$

により，証明は完了した。

3·6·6 G は Higman 群で，ϕ は G から G の中への同型写像とする。H

が G の benign な部分群であるならば，$\phi\upharpoonright H$ は benign である。

[証明] 3·6·1 により，ϕ は benign である。ゆえに，G_ϕ は Higman 群である。H が benign であるから，$(G_\phi)_H$ も Higman 群である。

ところで

$$\begin{aligned}(G_\phi)_H &= [G, s, t;\ sgs^{-1}=\phi(g),\ tht^{-1}=h]\\ &= [G, s, t, r;\ sgs^{-1}=\phi(g),\ stht^{-1}s^{-1}=\phi(h),\ r=st]\\ &= [G, r, s, t;\ rhr^{-1}=\phi(h),\ sgs^{-1}=\phi(g),\ t=s^{-1}r]\\ &= [G, r, s;\ rhr^{-1}=\phi(h),\ sgs^{-1}=\phi(g)]\\ &= (G_{\phi\upharpoonright H})_\phi\end{aligned}$$

すなわち，$G_{\phi\upharpoonright H}$ は Higman 群 $(G_\phi)_H$ にうめこめるから，やはり Higman 群である。

いま，G が Higman 群で，$\phi, \psi, \cdots$ が G の中の同型写像とする。このとき，集合 $\{\phi, \psi, \cdots\}$ が benign であるということを，$G_{\phi,\psi,\ldots}$ がある Higman 群 L にうめこめて，L の中で $\{t_\phi, t_\psi, \cdots\}$ が benign 部分群になっているようにできること，と定義する。

もし $\{\phi, \psi, \cdots\}$ が benign な $\phi_0, \psi, \cdots$ の有限集合であれば，$\{\phi, \psi, \cdots\}$ は benign である。これは，$G_{\phi,\psi,\ldots}$ が Higman 群になるから，これを L とおけば，$\{t_\phi, t_\psi, \cdots\}$ は有限個の生成元をもつから，3·6·2 により benign な部分群になっているからである。

3·6·7 G が Higman 群で，H は G の benign な部分群で，$\phi, \psi, \cdots$ は G の同型写像の benign な集合であるとする。いま，K が G の中の H を含み，$\phi, \psi, \cdots$ で不変な G の部分群の中で最小のものとする。このとき，K は benign な部分群である。

[証明] $\phi, \psi, \cdots$ が benign な集合であるから，Higman 群 L があって $G_{\phi,\psi,\ldots}\subseteq L$ で，L の中で $\{t_\phi, t_\psi, \cdots\}$ は benign であるとしてよい。

もし
$$K = G\cap\{H, t_\phi, t_\psi, \cdots\} \qquad (2)$$
を証明すれば，3·6·4 によって証明は完成する。

いま，ϕ, ψ, … の定義域をそれぞれ H_ϕ, H_ψ, … とすれば，$a \in H_\phi$ なる a に関しては

$$\phi(a)=t_\phi a t_\phi^{-1}$$

であるから

$$a \in \{H, t_\phi, t_\psi, \cdots\} \leftrightarrow \phi(a) \in \{H, t_\phi, t_\psi, \cdots\}$$

となり，(2)の右辺は ϕ で不変になる。K はこのようなものの最小であるから，つぎの式が得られる。

$$K \subseteq G \cap \{H, t_\phi, t_\psi, \cdots\}$$

一方，3·5·12 から

$$G \cap \{H, t_\phi, t_\psi, \cdots\} \subseteq G \cap \{K, t_\phi, t_\psi, \cdots\} = K$$

となるから，(2)は証明された。

さて，これまで‘部分群 H が benign である’というように benign を用いてきた。ここで，部分群とはかぎらない一般の部分集合に対して benign の定義を拡張したい。まず第1に，状況を整理して考えよう。A が有限集合であって，$[A]$ の任意の部分集合 P に関して‘P が benign である’ということを定義しようというのである。

まずその準備として，A に含まれない元 z をとってくる。いま，$X \in P$ について XzX^{-1} を考え，このような語全体から生成された $[A, z]$ の部分群を E_P と定義する。

3·1·13 によって，XzX^{-1} なる語の全体は $[A, z]$ で自由であるので

$$XzX^{-1} \in E_P \leftrightarrow X \in P$$

となり，E_P と P とはほとんど同じものと考えてよい。

そこで

‘P が $[A]$ で benign である’

を，つぎのように定義する。

‘E_P が $[A, z]$ で benign である’

P が $[A]$ の部分群であるときは

‘P が benign である’

という定義が二通りあることになるが，これについてはつぎの性質が成立する。

3·6·8 Pが $[A]$ の部分群であるときは，2つの benign の定義は一致する。

[証明] 最初に，Pが部分群として benign であったとする。このとき，3·6·4 により $\{P, z\}$ は $[A, z]$ の中で benign である。

さて，$E_{[A]}$ は z を含み，A の元による $[A, z]$ の内部同型で不変な最小な群であるから，3·6·7 により benign である。

つぎのことを証明しよう。

$$E_P=\{P, z\}\cap E_{[A]} \qquad (3)$$

これから，E_P が benign であることは 3·6·4 から出てくる。

明らかに

$$E_P\subseteq \{P, z\}\cap E_{[A]}$$

であるから，その逆

$$\{P, z\}\cap E_{[A]}\subseteq E_P$$

だけを証明すればよい。

さて，E_P は z を含み，Pの元による内部同型に関して不変である。したがって，$\{P, z\}$ の正規部分群である。したがって，$\{P, z\}/E_P$ は群となり，$\{P, z\}$ からこの群の上への surjective な準同型が与えられる。だから，$x\in\{P, z\}$ に対して，$x=py$, $p\in P$, $y\in E_P$ なる p, y が存在する。

$\phi: [A, z]\to[A]$ なる準同型を

$$\phi(a)=a, \qquad \phi(z)=e$$

と定義する。

このとき，$E_{[A]}$ は ϕ の核の中にはいっている。したがって，$x=py\in E_{[A]}$ のときは($p\in P$, $y\in E_P$ とする)

$$\begin{aligned}e&=\phi(x)=\phi(p)\phi(y)\\&=\phi(p)=p\end{aligned}$$

となるから $p=e$ で $x=y$, したがって $x\in E_P$ となって(3)がいえた。

つぎに，Pが部分集合として benign，すなわち E_P が benign と仮定して，

P が benign な部分群であることを証明しよう。

いま，新しい元 c, d をとってきて，A の任意の語 X に対して

$$\phi_X : \{c\} \to \{dX\}$$

を

$$\phi_X(c)=dX$$

によって定義する。ϕ_X は 3·6·1 により benign である。

われわれは，$\{\phi_X | X \in P\}$ が benign であることを証明する。

これが証明されたとすれば，c, d を含み，$\{\phi_X | X \in P\}$ のもとで不変な部分群は 3·6·7 により benign である。ところで，この群は明らかに $\{P, c, d\}$ であるから，$\{P, c, d\}$ は benign である。ところで

$$P=\{P, c, d\} \cap G$$

であるから，3·6·4 により P が benign であることが証明される。

さて，$\{\phi_X | X \in P\}$ が benign であることを証明するために，まず H を

$$H=[A, c, d]_{\phi_X, \phi_Y, \cdots}$$

によって定義する。ここに，X, Y, $\cdots$ は A のすべての語を走るものとする。

ϕ_X の定義にもどってかけば

$$H=[A, c, d, t_X, t_Y, \cdots ; t_X c t_X^{-1}=dX, \cdots]$$

ここでも，X, Y, $\cdots$ は A のすべての語を走るものとする。

$\{\phi_X | X \in P\}$ が benign であることを証明するためには，H をある Higman 群の中にうめこんで，$X \in P$ なる t_X の全体が生成する部分群が benign であるようにすればよい($\{\phi_X | X \in P\}$ が benign であることの定義である)。

いま，$A=\{a_1, \cdots, a_n\}$ としよう。

$$\psi_i : [A, c, d, t_X, t_Y, \cdots] \to [A, c, d, t_X, t_Y, \cdots]$$

なる自己同型写像を

$$\psi_i(a_j)=a_j, \qquad \psi_i(c)=c$$

$$\psi_i(d)=da_i, \qquad \psi_i(t_X)=t_{a_i X}$$

と定義する。

いま ψ_i を $t_X c t_X^{-1}=dX$ に施せば

$$t_{a_iX}ct_{a_iX}^{-1}=da_iX$$

となるから，ψ_i を H を定義する関係式に施せば，また H の関係式が出てくる。すなわち，$\psi_i \restriction H$ は H の自己同型写像になっている。

したがって，生成元が A, c, d, t_X (X は A の語)，a_1', …, a_n' であって，K をつぎの関係によって定義される群とすれば，H は K の中にうめこむことができる(ψ_i を a_i' による内部同型と考えればよい)。

$$t_Xct_X^{-1}=dX \quad (4)$$

$$a_i'a_ja_i'^{-1}=a_j \quad (5)$$

$$a_i'ca_i'^{-1}=c \quad (6)$$

$$a_i'da_i'^{-1}=da_i \quad (7)$$

$$a_i't_Xa_i'^{-1}=t_{a_iX} \quad (8)$$

いま，$t=t_e$, X' を，A の語 X の中の a_i をすべて a_i' にかえたものとすれば，(8)によりつぎの式が出てくる。

$$X'tX'^{-1}=t_X$$

さて，E_P は benign であると仮定したから

$$\begin{array}{ccc} [A,\, z] & \xrightarrow{z\text{を }t\text{ にかえる}} & K \\ \cup & & \cup \\ E_P & \longrightarrow & \{t_X,\ \cdots\} \end{array} \qquad (\text{ここで } X\in P)$$

を考えることにより，3·6·5 から $t_X=X'tX'^{-1}$ で生成される K の部分群は benign である。

ところで $X'tX'^{-1}=t_X$ であるから，t 以外の t_X は $X'tX'^{-1}$ でおきかえればよい。そうすると，(4)から

$$(X'tX'^{-1})c(X'tX'^{-1})^{-1}=dX \quad (4)'$$

が得られる。(4)を(4)′でおきかえれば，t 以外の t_X と(8)とをとり除いてよい。

ここで，(4)′は(5)，(6)，(7)と $tct^{-1}=d$ とから出てくることを証明しよう。

もしこれがいえたとすれば，$tct^{-1}=d$ は(4)の特別な場合であるから，K が有限表示群であることがいえて，H は K にうめこむことができ，そこで t_X

$(X \in P)$ 全体で生成される群は benign であることがいえるから，証明が完了したことになる。

ところで，(5), (6), (7)から

$$X'cX'^{-1}=c, \qquad X'dX'^{-1}=dX$$

がいえるから，$tct^{-1}=d$ から(4)$'$ は明らかである。

3·7 重要な補助定理

ここで重要な補助定理というのは，つぎの定理である。

補助定理 A が有限集合で，P は A の帰納的可算な語の集合であるとすれば，Pは benign である。

ここでPが帰納的可算というのは，もちろん3·4節におけるようにAの語に適当にゲーデル数を与えて，それぞれによって定義するのであるが，帰納的可算という概念がこのゲーデル数の与え方によらないことは明らかであろう。

まず最初に，この補助定理を仮定して，Novikoff–Boone の定理を導こう。このために，まず帰納的表示について定義しよう。

$G=[A; R]$ で A が有限で，R が帰納的可算であるときに，$[A; R]$ を G の**帰納的表示**という。帰納的表示がある群を**帰納的表示群**という。

$G=[A; R]$ で R が帰納的可算ならば，$C(R)$ は R から簡単な変形で導かれる関係の集合であるから，もちろん帰納的可算である。また，$C(R)$ が帰納的可算ならば，$G=[A; C(R)]$ となるから，もちろん G は帰納的表示群である。すなわち，$G=[A; R]$ が帰納的表示群であるというのは，$C(R)$ が帰納的可算であることと同等である。

有限表示群が帰納的表示群であることは明らかであろう(逆は成立しない)。

いま，Gが有限個の生成元 $x_1, \cdots, x_n$ をもっており，Gが有限表示群 $[B; S]$ にうめこめられたとする。このうめこみで，Gの生成元 $x_1, \cdots, x_n$ が表わすBの語をそれぞれ $X_1, \cdots, X_n$ とする。G で関係 ${x_{j_1}}^{i_1} \cdots {x_{j_n}}^{i_n}=e$ が成立するということは，$[B; S]$ で

$${X_{j_1}}^{i_1} \cdots {X_{j_n}}^{i_n}=e$$

が成立するということと同等である。すなわち

$$`x_{j_1}{}^{i_1}\cdots x_{j_n}{}^{i_n}=e \text{ が } G \text{ で成立する}' \leftrightarrow \ulcorner X_{j_1}{}^{i_1}\cdots X_{j_n}{}^{i_n}=e\urcorner \in C(S)$$

である。

いま，fを

$$\ulcorner X_{j_1}{}^{i_1}\cdots X_{j_n}{}^{i_n}=e\urcorner = f(\ulcorner x_{j_1}{}^{i_1}\cdots x_{j_n}{}^{i_n}=e\urcorner)$$

と定義すれば，fはもちろん帰納的可算である。したがって，$C(S)$ が帰納的可算であるから

$$f(\ulcorner x_{j_1}{}^{i_1}\cdots x_{j_n}{}^{i_n}=e\urcorner)\in C(S)$$

もやはり $\ulcorner x_{j_1}{}^{i_1}\cdots x_{j_n}{}^{i_n}=e\urcorner$ に関して帰納的可算である。したがって，Gが帰納的表示群であることがわかった。

まず，この事実の逆も成立することを補助定理を用いて証明する。これが，つぎの Higman の定理である。

Higman の定理：

Gが有限個の生成元をもっているとすれば，Gが有限表示群にうめこむことができる必要十分条件は，Gが帰納的表示群である。

[証明]　必要であることは上に述べたとおりであるから，十分であることのみを証明する。帰納的表示群は $\tilde{G}/K$ の形に表わされる。ここで，$\tilde{G}$ は有限個の元から生成される自由群であり，K は帰納的可算な $\tilde{G}$ の正規部分群である。

われわれの補助定理により，K は benign である。したがって，われわれは $\tilde{G}_K$ を有限表示群 H の中にうめこむことができる。

さて $\tilde{G}_K$ において，$\{\tilde{G}, t^{-1}\tilde{G}t\}$ は 3･5･6 により，$K=t^{-1}Kt$ を融合部分とする $\tilde{G}$ と $t^{-1}\tilde{G}t$ との融合積である。

ところで，$\tilde{G}$ から $\tilde{G}/K$ への準同型と $t^{-1}\tilde{G}t$ 全体を $\tilde{G}/K$ の単位元に移す準同型とは融合部分で一致するから

$$\phi:\{\tilde{G}, t^{-1}\tilde{G}t\}\to\tilde{G}/K$$

なる準同型を，つぎの条件で定義できる。

$$\phi(\tilde{g})=\tilde{g}/K,\qquad \phi(t^{-1}\tilde{g}t)=e/K$$

また

$$\psi : \{\tilde{G}, t^{-1}\tilde{G}t\} \rightarrow H\times(\tilde{G}/K)$$

なる同型写像を，つぎの条件で定義する。

$$\psi(x)=(x, \phi(x))$$

$\tilde{G}/K$ は $(H\times(\tilde{G}/K))_\psi$ の中にうめこむことができるから，定理を証明するためには，$(H\times(\tilde{G}/K))_\psi$ が有限表示群であることを証明すれば十分である。

$\tilde{G}_K\subseteq H$ で H は有限表示群であるから，もし必要ならばつけ加えることにして，H の有限表示の生成元の中に $\tilde{G}$ の生成元か t がもともとはいっているものとしてさしつかえない。

したがって，$(H\times(\tilde{G}/K))_\psi$ を表わすために，H の中の $\tilde{G}$ と $\tilde{G}/K$ の $\tilde{G}$ とを区別するために $\tilde{G}$ のコピー $\tilde{G}_1$ をつくり，これで $\tilde{G}/K$ の $\tilde{G}$ を表わして，その有限個の生成元を加え，ψ を内部同型で表わす元 s をつけ加える。

$(H\times(\tilde{G}/K))_\psi$ は，これらの生成元によってつぎの関係で表わされる。

H の関係　(1)

K_1 の元が e に等しいことを表わす関係　(2)

H の生成元が $\tilde{G}_1$ の生成元と交換可能であることを表わす関係　(3)

shs^{-1} を $\{\tilde{G}, t^{-1}\tilde{G}t\}$ の生成元 h に対して表わす関係　(4)

(1), (3), (4)は明らかに有限であるから，(2)が(1), (3), (4)から導かれることをいえば証明は終る。

いま，X_1 を $\tilde{G}_1$ の生成元の語で表わされた K_1 の元であるとする。このとき，$\phi(\tilde{g})=\tilde{g}/K$ を注意すれば，(4)から

$$sXs^{-1}=X\cdot X_1$$

が得られるはずである。また，さらに $\phi(t^{-1}\tilde{g}t)=e/K$ に注意すれば，(4)から

$$stXt^{-1}s^{-1}=X$$

も出てくるはずである。

ところで，X は K の元を表わすから，(1)より

$$tXt^{-1}=X$$

が出てくるはずである。この3つの式から，容易に

$$X = stXt^{-1}s^{-1}$$
$$= sXs^{-1} = X \cdot X_1$$

が出て，$X_1 = e$ が得られて証明が終った。

さて，この Higman の定理の応用として，3·4 節に述べた Novikoff–Boone の定理を証明することにしよう。

Novikoff–Boone の定理の証明

いま，Bを自然数の帰納的可算な集合であるが，帰納的ではない集合とする。$G = [a, b]$ として，G の部分群 H をつぎの生成元で生成される部分群とする。

$$a^n b a^{-n}$$

ここで，$n \in A$ に対してのみこの元を用いる。

ϕを H から H への恒等写像とすれば

$$G *_\phi G = [a, b, a_1, b_1;\ a^n b a^{-n} = a_1{}^n b_1 a_1{}^{-n} \text{ を } n \in A \text{ についてのみ用いる}]$$

となっている。したがって，$G *_\phi G$ は帰納的表示群である。

もし $a^n b a^{-n} = a_1{}^n b_1 a_1{}^{-n}$ が成立するとすれば，この元は $G \cap G_1$ に属する。ところで，$a^n b a^{-n}$ は 3·1·3 によりG で自由であるから，この元が H に属するのは $n \in A$ のときにかぎる。

この逆は明らかであるから，つぎの式が得られる。

$$a^n b a^{-n} = a_1{}^n b_1 a_1{}^{-n} \text{ が } G *_\phi G \text{ で成立している} \leftrightarrow n \in A$$

したがって，$G *_\phi G$ の語の問題が effective に解ければ，$a^n b a^{-n} = a_1{}^n b_1 a_1{}^{-n}$ が $G *_\phi G$ で成立するかどうかを判定する effective な方法があることになり，これは $n \in A$ を effective に決定する方法があることになって，Aが帰納的であるということになって矛盾する。

本章の残りで，本節のはじめに述べた補助定理の証明をするのであるが，本節の残りではそのために必要な補題のいくつかを証明する。今後，本節を通して，AおよびBは常に有限集合を表わすものとする。

3·7·1　すべての $[A]$ の有限部分集合は $[A]$ で benign である。

[証明] 3·6·2 より明らかである。

3·7·2 $A \subseteq B$ で，P が A の語の集合であるとき，P が $[A]$ で benign であれば，P は B でも benign である。

[証明] 3·6·3 より明らかである。

3·7·3 P, Q が $[A]$ の benign な部分集合とすれば，$P \cap Q$, $P \cup Q$ も $[A]$ の benign な部分集合である。

[証明] 3·1·13 により，XzX^{-1} の全体は自由であるので

$$E_{P \cap Q} = E_P \cap E_Q$$

$$E_{P \cup Q} = \{E_P, E_Q\}$$

が成立する。したがって，3·6·4 から明らかである。

いま，ϕ を $[A]$ から $[B]$ への写像とする。準同形 $\psi: [A, z] \to [B, z]$ が ϕ に**関連している**ということを

$$\psi(XzX^{-1}) = \phi(X)z\phi(X)^{-1}, \qquad X \in [A]$$

と定義する。

もし ϕ が準同型ならば，$\phi(z)=z$ とおいて ϕ を $[A, z]$ から $[B, z]$ への準同型に拡大できるので，ϕ は関連する準同型写像をもっている。

$[A]$ から $[A]$ への bijective な写像が nice であるということを，それが $[A, z]$ の自己同型である関連した写像をもっていること，と定義する。

明らかに 2 つの nice な写像の積は，また nice である。また，$[A]$ の自己同型 ϕ は $\phi(z)=z$ によって，$[A, z]$ の自己同型に拡大できるので nice である。

Y が A の語であるとき，$[A]$ から $[A]$ への写像 L_Y と R_Y をつぎの式で定義する。

$$L_Y(X) = Y \cdot X$$

$$R_Y(X) = X \cdot Y$$

L_Y と R_Y とは nice である。L_Y, R_Y にそれぞれ関連する自己同型 ϕ_1, ϕ_2 は，つぎの式で定義される。

$$\phi_1(W) = YWY^{-1}$$

$$\phi_2(a) = a$$

$$\phi_2(z)=YzY^{-1}$$

3·7·4　ϕ は $[A]$ から $[B]$ への写像で，関連した準同型をもっているとする。いま，P が $[A]$ で benign であるならば，$\phi(P)$ は B で benign である。

[証明]　ψ を ϕ に関連した準同型とすれば，つぎの式が得られる。

$$E_{\phi(P)}=\psi(E_P)$$

したがって，3·6·4 から証明される。

いま，P と Q とを $[A]$ の部分集合として，ϕ を $[A]$ から $[A]$ への写像とする。P が '(ϕ, Q)–不変である' ということを

$$\forall X\in Q(X\in P\leftrightarrow\phi(X)\in P)$$

と定義する。

P が '$(\phi, [A])$–不変である' ことを

'P が ϕ で不変'

という。

3·7·5　$P, Q_1, \cdots, Q_n$ は $[A]$ の benign な部分集合とする。さらに，$\phi_1, \cdots, \phi_n$ は $[A]$ から $[A]$ への nice な写像で，R は P を含み，$i=1, \cdots, n$ に対して (ϕ_i, Q_i)–不変なものの中で最小の $[A]$ の部分集合とする。このとき，R は benign である。

[証明]　ψ_i を ϕ_i に関連した $[A, z]$ の自己同型写像をする。3·6·6 により，$\psi_i\upharpoonright E_{Q_i}$ は benign である。したがって，3·6·7 により，E_P を含み $\psi_i\upharpoonright E_{Q_i}$ で不変な最小の部分群は benign である。

ゆえに，この最小の部分群が E_R であることを証明すれば十分である。

$g\in E_{Q_i}$ とすれば，g は $Xz^{\pm1}X^{-1}$ $(X\in Q_i)$ なる形の積で表わされるから，$\psi_i(g)$ はこの中の X を $\phi_i(X)$ でおきかえて得られる。

したがって，つぎの性質が成立する。

$$g\in E_R\leftrightarrow\psi_i(g)\in E_R$$

ゆえに，E_R は $\psi_i\upharpoonright E_{Q_i}$ のもとで不変である。

ところで，$E_P\subseteq E_R$ は明らかであるから，つぎの式が得られた。

$$(\text{上の条件を満たす最小の群}) \subseteq E_R$$

つぎに，この逆を考えるためにRがPから生成することを考えれば，これはPの元から，つぎの条件を満たすという仮定のもとで $\phi_1, \cdots, \phi_n, \phi_1^{-1}, \cdots, \phi_n^{-1}$ を何度か施して得られたものになっている。

Q_i の語になっているものにしか ϕ_i を施さない。

$\phi_i(Q_i)$ の語になっているものにしか ϕ_i^{-1} を施さない。

したがって，$X \in R$ ならば，XzX^{-1} は E_P を含んで $\phi_i \restriction E_{Q_i}$ で不変なすべての部分群に含まれていることがわかる。すなわち

$$E_R \subseteq (\text{上の条件を満たす最小の群})$$

がいえて，証明が完了した。

3·7·6 $P, Q_1, \cdots, Q_n$ は $[A]$ の benign な部分集合とする。さらに，$\phi_1, \cdots, \phi_n$ は $[A]$ から $[A]$ への nice な写像で，R はPを含み，ϕ_i-不変 $(i=1, \cdots, n)$ なるものの中で最小の $[A]$ の部分集合とする。このとき，R は benign である。

[証明] 3·7·5 において，$[A]$ 自身は benign な部分群，したがって部分集合であるからよい。

3·7·7 いま，$b_i = b^i a b^{-i}$ とおいて

$$P = \{b_{i_1}, b_{i_2}, \cdots b_{i_n} \mid 0 \leq i_1 < i_2 < \cdots < i_n\}$$

とおけば，Pは $[a, b]$ の benign な部分集合である。

[証明] H, H^+, H' をそれぞれ b_i 全体から生成された部分群，b_i $(i>0)$ 全体から生成された部分群，b_i $(i \geq 0)$ から生成された部分群とする。

まず，この3つの部分群が benign であることを証明する。

第1に，H はaを含み，bによってできる内部同型で不変である最小の部分群である。bによる内部同型が benign なことは，たとえば3·6·6によって明らかであるから，H は 3·6·7 によって benign である。

つぎに，H' は $H' = \{H^+, a\}$ であるから，もし H^+ が benign なことがわかれば，3·6·4 によって benign なことがわかる。したがって，H^+ が benign なことだけをいえばよい。

いま，$[a, b]$ から $[a, b]$ への2つの準同型を

$$\phi(a)=a, \qquad \phi(b)=b^2$$
$$\chi(a)=bab^{-1}, \qquad \chi(b)=b^2$$

によって定義しよう。

まず ϕ は injective である。このことは，$[a, b]$ の標準形の語に ϕ を施すとふたたび標準形の語が得られることから明らかであろう。

また，χ も injective である。これは $[a, b]$ の標準形の語に χ を施して，3・1節，(1)の変形だけで e になったとすると，最初に a が消えるところを調べてみれば，そのようなことがありえないことがただちにわかるから，明らかである。

ϕ も χ も injective であるから，3・6・6によって $\phi\restriction H$ と $\chi\restriction H$ は benign である。したがって，H^+ が benign なことをいうためには，3・6・7によって H^+ が b_1 を含み，$\phi\restriction H$ と $\chi\restriction H$ のもので不変な部分群の中で最小であることをいえばよい。

ところで

$$\phi(b_i)=\phi(b^i)a\phi(b^{-i})=b^{2i}ab^{-2i}=b_{2i}$$
$$\chi(b_i)=b^{2i}(bab^{-i})b^{-2i}=b_{2i+1}$$

となるから，b_1 を含んで $\phi\restriction H$ と $\chi\restriction H$ のもとで不変な部分群は $b_1, b_2, b_3, \cdots$ をすべて含むことは明らかである。

逆に，H の元 x は $b_i^{\pm 1}$ の積であり，この x が H^+ の元である必要十分条件は，この x をつくるために用いられた $b_i^{\pm 1}$ がいつでも $i>0$ を満たすということである(b_i の全体が3・1・13により自由であることに注意)。

このことから，容易につぎの式が得られる。

$$x \in H^+ \leftrightarrow \phi(x) \in H^+$$
$$\leftrightarrow \chi(x) \in H^+$$

これは，H^+ が $\phi\restriction H$ と $\chi\restriction H$ のもとで不変であることを意味する。

さて，さらに新しい $[a, b]$ の自己同型 ψ を

$$\psi(a)=bab^{-1}, \qquad \psi(b)=b$$

で定義しよう。

　このとき

$$\psi(b_i)=b^i\psi(a)b^{-i}$$
$$=b^{i+1}ab^{-(i+1)}=b_{i+1}$$

となる。われわれが証明したいこと‘P が benign である’をいうためには，3·7·5 により P が e を含み，(L_a, H^+)-不変で (ψ, H')-不変な部分集合の中で最小であることをいえばよい。

　まず，P が (L_a, H^+)-不変であることをいおう。

　H^+ の元は $b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}$ の形で，$0<i_1, \cdots, i_n$ である。したがって

$$L_a(b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1})=a\cdot b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}$$
$$=b_0b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}\qquad (b_0=a \text{ に注意})$$

b_i の全体は自由であるから，明らかにつぎの式が成立する。

$$b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}\in P\leftrightarrow b_0b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}\in P$$

　つぎに，P が (ψ, H')-不変であることをいおう。

　H' の元は $b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}$ の形で，$0\leq i_1, \cdots i_n$ である。

$$\psi(b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1})=b_{i_1+1}^{\pm1}\cdots b_{i_n+1}^{\pm1}$$

やはり，b_i 全体が自由であることから容易に

$$b_{i_1}^{\pm1}\cdots b_{i_n}^{\pm1}\in P\leftrightarrow b_{i_1+1}^{\pm1}\cdots b_{i_n+1}^{\pm1}\in P$$

が得られる。

　逆に，e を含んで，(L_a, H^+)-不変で，(ψ, H')-不変な部分集合があるとすれば

$$L_a(e)=a=b_0$$
$$\psi(b_0)=b_1,\ \psi(b_1)=b_2,\ \cdots,\ \psi(b_n)=b_{n+1},\ \cdots$$
$$L_a(b_{n+1})=b_0b_{n+1},\ \overbrace{\psi\cdots\psi}^{k}(b_0\,b_{n+1})=b_kb_{n+k+1}$$
$$L_a(b_{n+1}b_{n+k+2})=b_0b_{n+1}b_{n+k+2}\cdots$$

となって，すべての P の元を含むことは明らかである。

　$A=\{a_1, \cdots, a_n\}$ の語が正であるというのは，$a_1^{-1}, \cdots, a_n^{-1}$ を1つも含ん

でいないことであると定義する。

3・7・8 Aのすべての正な語の集合は benign である。

[証明] $A=\{a_1, \cdots, a_n\}$ として，$[A, z]$ の自己同型ϕをつぎの式によって定義する。

$$\phi(a_i)=a_{i+1} \qquad (i<n)$$
$$\phi(a_n)=a_1$$
$$\phi(z)=z$$

$[A, z]_\phi$ は 3・6・1 によって Higman 群である。G_ϕ において，ϕを内部同型で表わす元を t とすれば，$[a, b, z]$ から $[A, z]_\phi$ への準同型ψを，つぎの式で定義する。

$$\psi(a)=a_1$$
$$\psi(b)=t$$
$$\psi(z)=z$$

Pを 3・7・7 と同じように定義する。いま

$$\psi(b_0)=\psi(a)=a_1$$
$$\psi(b_1)=\psi(bab^{-1})=ta_1t^{-1}=a_2$$
$$\psi(b_k)=a_i \qquad (ここに，k\equiv i \pmod n で 1\leq i\leq n)$$

によって $\psi(P)$ はAのすべての正の語の全体の集合Qになることがわかる。したがって，$\psi(E_P)=E_Q$，したがって 3・6・5 と 3・7・7 とにより E_Q が benign であることがわかる。

3・8 補助定理の証明

さて，補助定理を順々に証明してゆくが，まず自然数のk重対を $\{a, b\}$ の語で表わすことを考えよう。

自然数の列 $x_1, x_2, \cdots, x_k$ に $a^{x_1}ba^{x_2}b\cdots ba^{x_k}$ を対応させる。この対応が自然数の有限列に対して，$[a, b]$ の元を1対1に対応させることは明らかであろう。

いま，自然数のk項関係 $R(x_1, \cdots, x_k)$ が benign であるということを，

集合

$$\{a^{x_1}ba^{x_2}b\cdots ba^{x_k}|R(x_1,\cdots,x_k)\}$$

が $[a, b]$ で benign であることと定義しよう。こうしてまず，いろいろな関係が benign であることを証明していって，最後に帰納的可算な関係が benign であることを証明してゆくことにする。

まずこの節では，W を $\{a, b\}$ の正の語の全体，W_b を W の語で b から始まる語の全体，i は有理整数を表わし，m と n は自然数を表わすものとする。

$W_b=L_b(W)$ であるから，3・7・8 と 3・7・5 とによって W も W_b もともに benign である。

3・8・1　2 項関係 $x_1=x_2$，3 項関係 $x_1+x_2=x_3$，$x_1\cdot x_2=x_3$ はすべて benign である。

［証明］　b を含み，L_aR_a のもので不変な最小の部分集合は明らかに a^iba^i の全体である。この集合と W との共通部分が a^nba^n の全体であるから，$x_1=x_2$ が benign であることがわかる。この a^nba^n 全体の集合を $S_=$ で表わすことにする。

さて，$L_b(S_=)$ を含み，L_aR_a で不変な最小の部分集合を考えれば，それは

$$ba^nba^n,\quad aba^nba^{n+1},\quad a^2ba^nba^{n+2},\quad \cdots,$$
$$-aba^nba^{n-1},\ -a^2ba^nba^{n-2},\ \cdots$$

の全体である。したがって，この集合とWとの共通部分がちょうど $x_1+x_2=x_3$ を表わす集合であるから，$x_1+x_2=x_3$ は benign である。

つぎに，$\{a, b, c\}$ の語を考えて，b を含み，L_aR_c で不変な最小の部分集合を考えれば，それは明らかに a^ibc^i の全体である。

したがって，この集合と $\{a, b, c\}$ の正な語との共通部分をとれば，a^nbc^n の全体の集合が得られる。この集合の L_{cb} による像を求めれば，cba^nbc^n の全体の集合が得られる。この集合をQとおこう。

いま，$[a, b, c]$ の自己同型ϕを

$$\phi(a)=a$$
$$\phi(b)=b$$

$$\phi(c)=ca$$

によって定義する。

いま，Qを含み，ϕで不変な最小の部分集合をつくれば，それは

$$ca^ iba^ nb(ca^ i)^ n$$

の全体の集合となる。したがって，この集合と正な語の集合との共通部分をつくれば，$ca^m ba^n b(ca^m)^n$ の全体の集合が得られる。これをPとおこう。

$[a, b, c]$ から $[a, b]$ への準同型ψを

$$\psi(a)=a$$

$$\psi(b)=b$$

$$\psi(c)=e$$

で定義する。

そうすれば，$\psi(P)$ は $a^m ba^n ba^{mn}$ 全体の集合であるから，$x_1\cdot x_2=x_3$ は benign である。

3·8·2　$P(x, x_1, \cdots, x_n)$ が benign で，$Q(x_1, \cdots, x_n, x)$ を

$$Q(x_1, \cdots, x_n, x) \leftrightarrow P(x, x_1, \cdots, x_n)$$

とすれば，$Q(x_1, \cdots, x_n, x)$ も benign である(benign の定義では，変数の順序も問題になることに注意せよ)。

[証明]　$P(x, x_1, \cdots, x_n)$ を表わす $\{a, b\}$ の語の集合をPとおこう。$n=0$ ならば明らかであるから，$n>0$ とする。

いま，$R_b(P)$ を含み，$L_{a^{-1}}R_a$ で不変な最小の部分集合を考えるとすれば，それは

$$a^{-i}Xba^i \qquad (X\in P)$$

なる語全体の集合である。

この集合と W_b との共通部分をとれば，Pは $a^x ba^{x_1}ba^{x_2}b\cdots ba^{x_n}$ なる形の語の集合であるから$(0\leq x, x_1, \cdots x_n)$

$$ba^{x_1}b\cdots ba^{x_n}ba^x$$

の全体の集合を得る。この集合に $L_{b^{-1}}$ を施せば

$$a^{x_1}b\cdots ba^{x_n}ba^x$$

の全体の集合を得る。したがって，$Q(x_1, \cdots, x_n, x)$ は benign である。

3・8・3 $P(x_1, \cdots, x_n)$ が benign であるとき，$Q(x, x_1, \cdots, x_n)$ を

$$Q(x, x_1, \cdots, x_n) \leftrightarrow P(x_1, \cdots, x_n)$$

で定義すれば，$Q(x, x_1, \cdots, x_n)$ も benign である。

［証明］ $L_b(P)$ を含み，L_a で不変な最小の部分集合を考えれば，それは

$$a^i b a^{x_1} b a^{x_2} \cdots b a^{x_n}$$

の全体の集合である。この集合と W との共通部分をとれば，Q を表わす集合が得られるから，Q は benign である。

3・8・4 $P(x, x_1, \cdots, x_n)$ が benign で，$Q(x_1, \cdots, x_n)$ を

$$Q(x_1, \cdots, x_n) \leftrightarrow \exists_x P(x, x_1, \cdots, x_n)$$

で定義すれば，$Q(x_1, \cdots, x_n)$ も benign である。

［証明］ P を含み，L_a で不変な最小の集合は，つぎの語の全体の集合となる。

$$a^{x+i} b a^{x_1} \cdots b a^{x_n}$$

これと W_b との共通部分をとって，$L_{b^{-1}}$ での像を求めればQを得る。

3・8・5 $P(x, x_1, \cdots, x_n)$ が benign で，$Q(x, x_1, \cdots x_n)$ を

$$Q(x, x_1, \cdots, x_n) \leftrightarrow \forall y < x P(y, x_1, \cdots, x_n)$$

で定義すれば，$Q(x, x_1, \cdots, x_n)$ も benign である。

［証明］ 3・8・3 により，すべての自然数の n 重対の集合は benign である。これに L_b を施すと，$R(x, x_1, \cdots, x_n) \leftrightarrow x=0$ なる $R(x, x_1, \cdots, x_n)$ が benign であることがわかる。この $R(x, x_1, \cdots, x_n)$ を表わす集合を R として，R を含んで (L_a, P)-不変な最小の集合を考えれば，それは

$b a^{x_1} \cdots b a^{x_n}$ を含んでいる

$a^i b a^{x_1} \cdots b a^{x_n}$ がこの集合とPとに含まれていれば

$a^{i+1} b a^{x_1} \cdots b a^{x_n}$ をつくる

$a^{i+1} b a^{x_1} \cdots b a^{x_n}$ がこの集合とPとに含まれていれば

$a^i b a^{x_1} \cdots b a^{x_n}$ をつくる

によって得られる集合である。これと W との共通部分をつくれば，この集合

が $Q(x, x_1, \cdots, x_n)$ を表わすことは明らかである。

3・8・6　$j_1, \cdots, j_k$ が $1, \cdots, n$ の部分列で，$P(x_{j_1}, \cdots, x_{j_n})$ が benign であるとき，$Q(x_1, \cdots, x_n)$ をつぎの式で定義すれば

$$Q(x_1, \cdots, x_n) \leftrightarrow P(x_{j_1}, \cdots, x_{j_n})$$

$Q(x_1, \cdots, x_n)$ は benign である。

[証明]　$Q(x_1, \cdots, x_n) \leftrightarrow \exists y_1 \cdots y_k(y_1=x_{j_1} \wedge \cdots \wedge y_k=x_{j_k}$

$$\wedge P(y_1, \cdots, y_k))$$

ところで，$y_1, \cdots, y_k, x_1, \cdots, x_n$ の命題としてみたとき，$y_i=x_{j_i}$ は 3・8・2 と 3・8・3 とにより benign である。$P(y_1, \cdots, y_k)$ も同様にして benign であることがわかる。よって，証明は 3・7・3 と 3・8・4 によって容易に得られる。

3・8・7　$x=n$ は x の命題として benign である。

[証明]　3・7・1 より明らかである。

3・8・8　$f(x_1, \cdots, x_n)$ が帰納的であるとき，$f(x_1, \cdots, x_n)=x$ は benign である。

[証明]　f が $f(x_1, \cdots, x_n)=x_i$ で定義されているときは，3・8・1，3・8・2，3・8・3 から明らかである。

f が $+$ か $\cdot$ のときは，3・8・1 より明らかである。

つぎに，$x \neq 0$ が benign なことは，$a^{n+1}b$ が $a^n b$ の L_a による像であり，3・8・3 から明らかに $a^n b$ の全体が benign であることから導かれる。

つぎに，$\leq$ と $<$ が2項関係として benign なことは

$$x \leq y \leftrightarrow \exists z(x+z=y)$$

$$x<y \leftrightarrow \exists z(z \neq 0 \wedge x+z=y)$$

から明らかである。

いま，$f(x, y)$ が $x<y$ の特性関係，すなわち $x<y$ が成立しているときは 0, そうでないときは1を表わすものとすれば，$f(x, y)=z$ が benign であることは，つぎの式からわかる(3・7・3 に注意)。

$$f(x, y)=z \leftrightarrow (x<y \wedge z=0) \vee (y \leq x \wedge z=1)$$

つぎに，$f(x_1, \cdots, x_n)$ が帰納的な関数 $g, h_1, \cdots, h_k$ から

$$f(x_1, \cdots, x_n)=g(h_1(x_1, \cdots, x_n), \cdots, h_k(x_1, \cdots, x_n))$$

で定義されていて，g, h_1, $\cdots$, h_k に対してはすでに証明されているとすれば，$f(x_1, \cdots, x_n)=x$ が benign であることは

$$f(x_1, \cdots, x_n)=x \leftrightarrow \exists y_1 \cdots y_k(h_1(x_1, \cdots x_n)=y_1 \wedge \cdots \wedge h_k(x_1, \cdots, x_n)=y_k \wedge g(y_1, \cdots, y_k)=x)$$

から容易にわかる。

つぎに，$f(x_1, \cdots, x_n)=\mu x(g(x_1, \cdots, x_n, x)=0)$ で f が帰納的な g から定義されて，g に対してはすでに証明がされているときは

$$f(x_1, \cdots, x_n)=x \leftrightarrow g(x_1, \cdots, x_n, x)=0 \wedge \forall y<x \exists z(z \neq 0 \wedge g(x_1, \cdots, x_n, x)=z)$$

となるから $f(x_1, \cdots, x_n)=x$ が benign であることがわかる。

以上から，1·4 節の定理 1 により証明が完了する。

3·8·9 $P(x_1, \cdots, x_n)$ が帰納的可算ならば，$P(x_1, \cdots, x_n)$ は benign である。

［証明］ 3·8·4 から，P が帰納的なときを証明すれば十分である。ところで，P の特性関数を f とすれば，f は帰納的であるから $f(x_1, \cdots, x_n)=x$ は benign, ゆえに $\exists x(x=0 \wedge f(x_1, \cdots, x_n)=x)$ は benign で証明された。

3·8·10 A は有限集合で，Q は A の上の帰納的可算な正の語の集合とすれば，Q は benign である。

［証明］ いま，P を 3·7·7 における P とする。すなわち，$b_i=b^i a b^{-i}$ で

$$P=\{b_{i_1} b_{i_2} \cdots b_{i_n} | 0 \leq i_1 < i_2 < \cdots < i_n\}$$

さらに，3·7·8 の証明と同じように $[a, b, z]$ から $[A, z]_\phi$ への準同型 ϕ を定義すれば，3·7·8 の証明から $\phi(P)$ が A の正の語の全体となる。

Q は正な語の集合であるから

$$\phi(\phi^{-1}(Q) \cap P)=Q$$

となり，ゆえに

$$\phi(E_{\phi^{-1}(Q) \cap P})=E_Q$$

となるから，$\phi^{-1}(Q) \cap P$ が benign であることを証明すればよい。

ところで，$\phi^{-1}(Q)\cap P$ は明らかに帰納的可算であるから，P のすべての帰納的可算な部分集合が benign であることを証明すれば十分である。

いま，$[a, z]$ から $[a, z]$ への準同型 ϕ をつぎの式で定義する。

$$\phi(a)=a^2$$

$$\phi(z)=z$$

明らかに ϕ は injective である(3・7・7 で証明した)。3・6・1 により，$[a, z]_\phi$ は Higman 群である。

$[a, z]_\phi$ において，その内部同型により ϕ を表わす元を t として，χ を $[a, b, z]$ から $[a, z]_\phi$ への $\chi(b)=t$ によって定義される準同型とする。

$b_i=b^iab^{-i}$ を用いれば

$$\begin{aligned}\chi(b_i)&=\chi(b^i)\chi(a)\chi(b^{-i})\\&=t^iat^{-i}=\overbrace{\phi(\cdots\phi}^{i}(a)\cdots)\\&=a^{2^i}\qquad(i\geq 0)\end{aligned}$$

したがって，$X=b_{i_1}\cdots b_{i_n}\in P$ とすれば

$$\chi(X)=a^x\qquad(ここで\ x=2^{i_1}+\cdots+2^{i_n})$$

したがって

$$\chi(XzX^{-1})=a^xza^{-x}$$

が得られる。

ところで，正の自然数を $2^{i_1}+\cdots+2^{i_n}$ $(0\leq i_1<\cdots<i_n)$ の形にかくかき方はただ一通りであるから，χ は E_P の上で injective である。ゆえに

$$E_R=E_P\cap\chi^{-1}(\chi(E_R))$$

これから，$\chi(E_R)$ が benign であることを証明すれば十分である。

ところで，$\chi(XzX^{-1})=a^xza^{-x}=\chi(X)z\chi(X^{-1})$ から

$$\chi(E_R)=E_{\chi(R)}$$

ここに，$\chi(R)$ は a の正の語の集合である。しかも，R が帰納的可算であるから，$\chi(R)$ も帰納的可算である。ゆえに，3・8・9 により $\chi(R)$ は benign であることがわかって，証明が終った。

さて，つぎにいよいよ補助定理の証明をすることにする。

補助定理の証明

ふたたび P を有限集合 $A=\{a_1, \cdots, a_n\}$ の帰納的可算な語の集合とする。いま，$A'=\{a_1', \cdots, a_n'\}$ として，$[A, A']$ から A への準同型 ϕ をつぎの式で定義する。

$$\phi(a_i)=a_i$$

$$\phi(a_i')=a_i^{-1} \qquad (i=1, \cdots, n)$$

P' を $A\cup A'$ の正な語 X で $\phi(X)\in P$ なるものの全体とすれば，P' は帰納的可算で，3・8・10 により benign である。$P=\phi(P')$ であるから，P は 3・7・4 により benign である。

参考文献

第1章帰納的関数についての文献は数多くあるが，ここではつぎの2つの本だけをあげておく。

S. C. Kleene: *Introduction to Mathematics*, D. van Nostrand Co., Princeton, 1952.

H. Rogers, Jr.: *Theory of Recursive Functions and Effective Conputability*, McGraw-Hill, New York, 1967.

これ以上のこの分野の文献は，この両著書の巻末の文献表をみられたい。前者はこの分野を実質的に大成させた人自身の著書であり，後者はかなり辞書的な本である。

第2章の文献としては，まず

Ju. V. Matijasevič: Enumerable sets are diophantine, *Dokl. Akad. Nauk SSSR*, **191** (1970), p. 279-282.

がある。また，それ以前の仕事については

M. Davis, H. Putnam & J. Robinson: The Decision Problem for Exponential Diophantine Equations, *Ann. of Math.*, vol. 74 (1961), pp. 425-436.

および

M. Davis: *Computability & Unsolvaility*, McGraw-Hill, New York, 1958.

をみられたい。

Pell の方程式については

高木貞治：初等整数論講義(第2版)，共立出版，1971.

がよいと思う。

第3章の文献としては，まず自由群論については

彌永昌吉：自由群論，大阪大学数学講座集，岩波書店，1941.

A. G. Kurosh: *The Theory of Groups*, vol. 2, Chelsea, New York, 1956.

がよいと思う。後者はもちろん，ロシヤ語本の英訳である。

Novikoff, Boone の定理については

P. S. Novikoff: On the algorithmic unsolvability of the word problem in groups (Russian), *Trudy Mat. Inst. Steklov* no. 44, Izdat Akad. Nauk SSSR, Moscow, 1955.

W. W. Boone: The word problem, *Ann. of Math.*, **70** (1959), p. 207–265.

この両者の証明に比べて，つぎの証明はわかりやすい。

J. L. Britton: The word problem, *Ann. of Math.*, **77** (1963), p. 16–32.

Higman の定理については

C. Higman: Subgroups of infinitely presented groups, *Proc. of Royal Soc.* Series A, vol. 262 (1961), p. 455–475.

をみられたい。

このほか，この章に関係のあるおもな著書および論文として，つぎの 4 つをあげておきたい。

C. F. Miller, III: On Group-Theoretic Decision Problems and Their Classification, *Ann. of Math. Studies*, Princeton Univ. Press, Princeton, 1971.

M. O. Rabin: Recursive unsolvability of group theoretic problems, *Ann. of Math.*, **67** (1958), p. 172–194.

J. J. Rotman: *The Theory of Groups*, Allyn and Bacon, Bacon, Boston, 1965.

J. R. Shoenfield: *Mathematical Logic*, Addison-Wesley, Reading, Mass., 1967.

索　引

B

benign　87
　部分群 H が——　87
　部分集合 P が——　91
　同型写像 ϕ が——　87
　$R(x_1, \cdots, x_k)$ が——　104
　集合 $\{\varphi, \psi, \cdots\}$ が——　90
Boone-Novikoff の定理　82
部分　69
部分群 H が benign　87
部分集合 P が benign　91
ブロック　69

C

Chinese remainder theorem　3
Church の thesis　16
closed である　34

D

第10問題(ヒルベルトの)　42
Davis, M.　43
diophantine　25
　広い意味で——　25
　——な命題　43
同型写像 ϕ が benign　87

E

effective な解法(語の問題の)　17, 81

G

ゲーデル数　29
原始帰納的関数(primitive recurcive function)　6
語　67
　——$b_1 \cdots b_i$ が標準形　69
　——が正規　75
　——の長さ　67
語の問題　17
　——の effective な解法　81
g と h から I で定義される関数　5
群 G の中で自由　72

H

Higman 群　82
Higman の定理　96
広い意味で diophantine　25
ヒルベルトの第10問題　42
表示　80
標準形(語の)　69

I

一様　69

K

関係のある群　73
関連している　99
計算できる(effective)　17
決定問題　39
帰納的表示　95
帰納的表示群　95
帰納的関数(recursive function)　16
帰納的可算(recursive enumarable)　22, 24
Kleene の T　39

M

Matijasevič, Ju. v.　43
命題
　diophantine な——　43

$Q_1, \cdots, Q_m$ が互いに相反する——　11
初等的な——　24, 43
文字　67

N

Novikoff-Boone の定理　82

P

Pell の方程式　46
Putnam, H.　43

Q

$Q_1, \cdots, Q_m$ が互いに相反する命題　11
$Q_1, \cdots, Q_m$ の場合に分けて，φ を $\varphi_1, \cdots, \varphi_{m+1}$ で定義する　11

R

Robinson, J.　43
$R(x_1, \cdots, x_k)$ が benign　104

S

正規(語が)　75
初等的な命題　24, 43
集合 $\{\varphi, \psi, \cdots\}$ が benign　90

T

互いに相反する命題　11
特性関数　9
truth definition　36

Y

有限表示群　80
融合部分　75
融合積　75, 80

Z

自由(群の中で)　72
自由 Abel 群　71
自由群　67, 69
自由積　79
剰余定理　3

記 号 一 覧

第1章　帰納的関数

$\neg$（でない）　1
$\wedge$（そして）　1
$\vee$（または）　1
$\rightarrow$（ならば）　1
$\forall$（すべて）　1
$\exists$（存在する）　1
$\leftrightarrow$（同値）　1
$a|b$（a が b を割る）　2
$a \nmid b$（上の否定）　2
(a, b)（a と b との最大公約数）　2
$\langle a, b\rangle$（順序対）　3
$a \equiv b \pmod{c}$　3
$J(a, b)$　5
$a+b$　6
$a \cdot b$　7
a^b　7
$a!$　7
$a \dot{-} 1$　7
$a \dot{-} b$　7
$\min(a, b)$（a と b との小さいほう）　7
$\min(a_1, \cdots, a_n)$（$a_1, \cdots, a_n$ の最小）　7
$\max(a, b)$（a と b との大きいほう）　7
$\max(a_1, \cdots, a_n)$（$a_1, \cdots, a_n$ の最大）　8
$\mathrm{sg}(a)$　8
$\overline{\mathrm{sg}}(a)$　8
$|a-b|$　8
$[a/b]$（a を b で割ったときの商）　8
$\sum_{y<z} f(x_1, \cdots, x_n, y)$　8
$\prod_{y<z} f(x_1, \cdots, x_n, y)$　9
$a=b$　9
$\mu y P(y)$　10
$Pr(a)$（a が素数）　12
p_i（$(i+1)$ 番目の素数）　12
$(a)_i$　12
$\mathrm{lh}(a)$（a の長さ）　12
$a * b$　13
$\tilde{f}$　13
F　18
$\ulcorner A \urcorner$（A のゲーデル数）　29
$\mathrm{pol}(x)$　30
$\mathrm{Pol}(x)$　30
$n(i)$　30
$\mathrm{Nl}(x)$　30
$\mathrm{plsub}\left(\binom{b}{c} x\right)$　31
$\mathrm{varpl}(b, x)$　32
$\mathrm{Varpl}(b, x)$　32
$\mathrm{Atom}(x)$　32
$\mathrm{atsub}\left(\binom{b}{c} x\right)$　33
$\mathrm{Varat}(b, x)$　33
$\mathrm{Form}(x)$　34
$\mathrm{Clpl}(x)$　34
$\mathrm{Clat}(x)$　34
$\mathrm{Clfm}(x)$　34
$\mathrm{fmsub}((2/c), x)$　35
$\mathrm{Val}(x)$　36
$\mathrm{Trat}(x)$　37
$l(i, n)$　37
$\mathrm{Tr'fm}(x)$　38
$\mathrm{Tr}(x)$　38
$T(e, k, b)$　38

第2章 ヒルベルトの第10問題

$x_n(a)+y_n(a)\sqrt{a^2-1}$ 47

第3章 群の語の問題

$[A]$ (自由群) 69
$G*_{\phi}G'$ (G, G' の ϕ による融合積) 75
$G*G'$ (G と G' との自由積) 79
$[A;R]$ (G の表示) 80
$R(x_1, \cdots, x_k)$ (自然数の k 項関係) 104

竹内外史 略歴

1926年 石川県に生まれる
1947年 東京大学理学部数学科卒
1956年 理学博士
現　職 イリノイ大学教授

主要著書

数学基礎論 (共立出版)
現代集合論入門 (日本評論社)
数学基礎論の世界 (日本評論社)

昭和48年4月20日 初版発行

数理科学シリーズ 7
数理論理学
—語の問題—

著　者 竹内外史
発行者 山本健二

発行所 株式会社 培風館
東京都千代田区九段南4-3-12・郵便番号102
電話(03) 262-5256 (代表)・振替東京44725

定価 ¥1500.

日東紙工印刷・三水舎製本

著者の承認をえて検印を省略しました

3341-0607-6955